COPYRIGHT AND CITATION CONSIDERATIONS FOR THIS THESIS/DISSERTATION

This copy has been supplied on the understanding that it is copyrighted and that no quotation from the thesis may be published without proper acknowledgement.

Please include the following information in your citation:

- Name of author
- Year of publication, in brackets
- Title of thesis, in italics
- Type of degree (e.g. D. Phil.; Ph.D.; M.Sc.; M.A. or M.Ed. …etc.)
- Name of the University
- Website
- Date, accessed

Example

Governance responses to hacking in the banking sector of South Africa: An exploratory study

by

Christiaan J. Roos

THESIS

Submitted in fulfillment of the requirements for the degree

DOCTOR COMMERCII

in

AUDITING

in the

FACULTY OF ECONOMIC AND FINANCIAL SCIENCES

at the

University of Johannesburg

Supervisor: Professor Doctor T. L. Voogt
Co-supervisor: Professor Doctor B. Marx

November 2012
ABSTRACT

Organisations today are critically dependent on IT to enable business operations and ensure competitiveness in a growing international marketplace. At the same time, IT also introduces significant risks, such as hacking. The board of directors is ultimately responsible for mitigating IT risk as a component of business risk. This task is included in its corporate governance responsibilities, which, in the South African context, is underpinned by the King Code of Corporate Governance. The board of directors also plays a key role in identifying and enabling the most appropriate responses to IT risk, including hacking. This inevitably necessitates greater focus on and understanding of risks such as hacking.

The determined and elusive nature of hackers makes them a significant threat to organisations today. Not only are hackers characterised by various profiles and motives, but they are also exceptionally skilled in exploiting weak security practices and software vulnerabilities, with attack techniques which range from non-technical social engineering to advanced technical attacks and exploits. Hackers are role-players in cybercrime and cyber warfare, as is evident from the media and information security survey results explored in this thesis, in particular within the banking sector, which is the financial backbone of the country. It is for this reason that the South African banking sector has been selected as the target population for this study.

This study considers the meaning and nature of hacking, viewing it as either a risk or an event, which requires preventative or detective responses. The effect of hacking on business risks is explored next by identifying common business risks and common IT risks themes, where after the fundamental links between hacking and the IT risk themes are established. This study further argues that business risks are increased by IT risks, which implies that, by indirect association, business risks are increased by hacking. A response to this threat is required, in particular from a governance perspective, with the board of directors playing a fundamental role in supporting the appropriate responses. This study explores the advantages and disadvantages of various responses to hacking, highlighting the point that most traditional responses are not effective enough in fully mitigating the hacking threat. It is argued that ethical hacking is an effective response to the threat of hacking. The nature of ethical hacking is explored, including its objectives, motivation, advantages and disadvantages. The multi-faceted nature of the ethical hacking response is also considered.
In order to explore the risks and responses to hacking in the banking sector in South Africa, an analysis of annual reports was conducted and two questionnaires were administered. The analysis of the annual reports of the 16 locally registered banks in South Africa highlighted differences in disclosure practices around IT risk, IT governance and hacking. This was followed by empirical testing in the local banking sector, by using a mixed-method approach in order to solicit mostly quantitative, but also qualitative, responses from company secretaries and individuals responsible for IT at the 16 locally registered banks.

The results of the questionnaires indicated that the board of directors is not fully embracing its IT governance responsibilities and that IT matters are mostly dealt with by risk management committees at board level or IT steering committees at executive management level. The effect of IT risks on business risks such as human resource risk and physical risk is underestimated. Respondents were unclear about the effect of hacking on IT risks, such as IT human resource risk and lack of software development. The local banking sector is not fully aware of how hacking can affect organisations, and banks are not making enough use of ethical hacking as a response to the hacker threat.

This is the first study of its kind to explore ethical hacking in the context of governance responses. The study breaks new ground by providing a unique in-depth analysis of the link between business risk, IT risk and hacking. It is also the first study into the various responses to hacking in the SA banking sector and will assist not only the banking industry but business at large in defining appropriate preventative and detective responses to hacking.

Key words:

board of directors, corporate governance, IT governance, business risk, IT risk, hackers, hacking, ethical hacking, banking sector
“Above the comforts of Base Camp, the expedition in fact became an almost Calvinistic undertaking. The ratio of misery to pleasure was greater by order of magnitude than any other mountain I’d been on; I quickly came to understand that climbing Everest was primarily about enduring pain. And subjecting ourselves to week after week of toil, tedium, and suffering, it struck me that most of us were probably seeking, above all else, something like a state of grace.”

Jon Krakauer

Into thin air
ACKNOWLEDGEMENTS

The mammoth task of completing a doctoral study does not take place without the help of various individuals:

• First of all, I want to thank my supervisor, Prof Thea Voogt, for her unwavering diligence in providing meticulous feedback and guidance on every submission. Her depth and breadth of knowledge is extraordinary. Undoubtedly, she contributed significantly towards the successful completion of my thesis.

• Secondly, to my co-supervisor, Prof Ben Marx, for his timely advice, encouragement and guidance.

• Thirdly, I want to thank Prof Alex van der Watt, for his earlier contributions to my study and financial support granted by the UJ Department of Accountancy.

• Also thank you to Prof Dempsey, for her support in allowing me to complete my studies.

• My gratitude also goes to Adam Martin for the design of the questionnaire website and Prof Craig McKenzie for the language editing.

• I also want to thank the general staff, such as library staff, research assistants, other academic staff of the University of Johannesburg who have assisted me.

• I want to thank my friends and family for their support. In particular, I want to thank my father, Christaan Roos, who financed my very first degree and set me off on this academic expedition, which I have now successfully completed.

• Of course, I also want to thank my wife, Mar-Zanne Roos and my son, Alvin Roos, for their love, support and patience whilst I completed this expedition. I hope I can make up for the lost time.

• Finally, I want to thank my Heavenly Father for always being the light in the times of darkness and for Jesus Christ, our ultimate saviour.
## INDEX

<table>
<thead>
<tr>
<th>Abstract</th>
<th>i</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acknowledgements</td>
<td>iv</td>
</tr>
<tr>
<td>Index</td>
<td>v</td>
</tr>
<tr>
<td>List of tables</td>
<td>xxii</td>
</tr>
<tr>
<td>List of figures</td>
<td>xxvi</td>
</tr>
<tr>
<td>List of picture</td>
<td>xxvi</td>
</tr>
<tr>
<td>Abbreviations</td>
<td>xxvii</td>
</tr>
</tbody>
</table>

### CHAPTER 1

**INTRODUCTION AND STUDY LAYOUT**

<table>
<thead>
<tr>
<th>1.1 INTRODUCTION</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2 RESEARCH PROBLEM</td>
<td>6</td>
</tr>
<tr>
<td>1.3 MOTIVATION FOR THE STUDY</td>
<td>6</td>
</tr>
<tr>
<td>1.4 RESEARCH OBJECTIVES</td>
<td>6</td>
</tr>
<tr>
<td>1.5 BENEFITS AND APPLICATION OF THE STUDY</td>
<td>8</td>
</tr>
<tr>
<td>1.6 SCOPE OF THE STUDY</td>
<td>8</td>
</tr>
<tr>
<td>1.7 LIMITATIONS OF THE STUDY</td>
<td>9</td>
</tr>
<tr>
<td>1.8 STUDY LAYOUT</td>
<td>10</td>
</tr>
<tr>
<td>1.8.1 Introduction and study layout (Chapter 1)</td>
<td>11</td>
</tr>
<tr>
<td>1.8.2 The changing face of IT in business (Chapter 2)</td>
<td>11</td>
</tr>
<tr>
<td>1.8.3 Investigating the meaning and nature of hacking (Chapter 3)</td>
<td>11</td>
</tr>
<tr>
<td>1.8.4 Hacking within the context of business risk (Chapter 4)</td>
<td>12</td>
</tr>
<tr>
<td>1.8.5 Responses to hacking (Chapter 5)</td>
<td>12</td>
</tr>
<tr>
<td>1.8.6 The ethical hacking response (Chapter 6)</td>
<td>12</td>
</tr>
<tr>
<td>1.8.7 Banking in South Africa (Chapter 7)</td>
<td>13</td>
</tr>
<tr>
<td>1.8.8 Description of the research methodology (Chapter 8)</td>
<td>13</td>
</tr>
<tr>
<td>1.8.9 Research findings and recommendations (Chapter 9)</td>
<td>13</td>
</tr>
<tr>
<td>1.8.10 Conclusion, recommendations and further areas of research (Chapter 10)</td>
<td>13</td>
</tr>
</tbody>
</table>

| 1.9 THEMATOLOGICAL QUESTIONS | 13 |

**Index**

| 1.9 THEMATOLOGICAL QUESTIONS | 13 |
# CHAPTER 2
## THE CHANGING FACE OF IT IN BUSINESS

2.1 INTRODUCTION

2.2 REFLECTING ON THE HISTORY OF IT IN BUSINESS PRIOR TO THE 1980s

2.3 REFLECTING ON THE HISTORY OF IT IN BUSINESS DURING THE 1980s

2.4 REFLECTING ON THE HISTORY OF IT IN BUSINESS SINCE THE 1990S AND BEYOND

2.5 THE PERVERSIVE IMPACT OF IT ON BUSINESS TODAY

2.6 IT GOVERNANCE

2.7 CHAPTER SUMMARY

# CHAPTER 3
## INVESTIGATING THE MEANING AND NATURE OF HACKING

3.1 INTRODUCTION

3.2 THE ORIGINS, EVOLUTION AND MEANING OF HACKING

3.2.1 Introduction

3.2.2 Historical origins of the terms “hacker” and “hacking” in brief

3.2.3 The evolution of hackers and the hacking culture

3.2.4 Defining “hackers” and “hacking”

3.2.5 The change in meaning of the words “hacker” and “hacking”

3.2.6 Conclusion

3.3 HACKER PROFILES

3.3.1 Introduction

3.3.2 Script kiddies

3.3.3 Crackers

3.3.4 Über hackers

3.3.5 Black hat hackers
<p>| 3.3.6 | White hat hackers | 47 |
| 3.3.7 | Grey hat hackers | 49 |
| 3.3.8 | The resultant two dimensions of hackers | 50 |
| 3.3.9 | Conclusion | 52 |
| <strong>3.4</strong> | SOURCES HACKERS USE TO ACQUIRE THEIR SKILLS | 53 |
| <strong>3.5</strong> | IDENTIFYING HACKER MOTIVES, OBJECTIVES AND ETHICAL VIEWPOINTS | 54 |
| 3.5.1 | Introduction | 54 |
| 3.5.2 | General psychology and underlying motives of hackers | 55 |
| 3.5.3 | Specific objectives of hackers | 59 |
| 3.5.3.1 | Hackers engaging in extortion or pursuing organised crime | 59 |
| 3.5.3.2 | Hackers engaging in hacktivism | 60 |
| 3.5.3.3 | Hackers engaging in vigilantism | 61 |
| 3.5.3.4 | Hackers engaging in industrial espionage | 61 |
| 3.5.3.5 | Hackers engaging in terrorism | 62 |
| 3.5.3.6 | The objectives of hackers who find themselves inside organisations | 63 |
| 3.5.4 | Conclusion | 66 |
| <strong>3.6</strong> | A COMMON HACKER METHODOLOGY | 67 |
| <strong>3.7</strong> | BASIC HACKING TOOLS AND TECHNOLOGIES USED BY HACKERS | 69 |
| <strong>3.8</strong> | WEAKNESSES THAT FACILITATE SUCCESSFUL HACKING ATTEMPTS | 71 |
| 3.8.1 | Introduction | 71 |
| 3.8.2 | Identifying broad categories of weaknesses that facilitates hacker attacks | 72 |
| 3.8.3 | Weaknesses associated with physical access | 73 |
| 3.8.3.1 | Hackers obtaining physical access to a premises | 73 |
| 3.8.3.2 | Hackers circumventing physical access by accessing mobile computing devices | 74 |
| 3.8.3.3 | Hackers circumventing physical access via wireless networks | 75 |
| 3.8.4 | Weaknesses associated with logical access controls | 76 |
| 3.8.5 | Software and hardware vulnerabilities | 78 |
| 3.8.6 | Global interconnectedness of networks | 81 |
| 3.8.7 | The human factor | 83 |
| 3.8.8 | Conclusion | 85 |
| <strong>3.9</strong> | HACKER TECHNIQUES | 86 |</p>
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.1</td>
<td>General hacker techniques from selected sources on hacking</td>
<td>87</td>
</tr>
<tr>
<td>3.9.1.1</td>
<td>General hacker techniques by Skoudis and Liston</td>
<td>87</td>
</tr>
<tr>
<td>3.9.1.2</td>
<td>General hacker techniques by Harding</td>
<td>92</td>
</tr>
<tr>
<td>3.9.2</td>
<td>Hacker techniques defined in ethical hacking qualifications</td>
<td>93</td>
</tr>
<tr>
<td>3.9.3</td>
<td>Hacker techniques for web application attacks</td>
<td>95</td>
</tr>
<tr>
<td>3.9.4</td>
<td>Hacking techniques of a non-technical nature</td>
<td>97</td>
</tr>
<tr>
<td>3.9.5</td>
<td>Hacker techniques defined by the IT Governance Institute</td>
<td>98</td>
</tr>
<tr>
<td>3.9.6</td>
<td>Other general hacker techniques</td>
<td>99</td>
</tr>
<tr>
<td>3.10</td>
<td>HACKING: A TYPE OF CYBERCRIME</td>
<td>100</td>
</tr>
<tr>
<td>3.10.1</td>
<td>Cybercrimes committed by hackers</td>
<td>101</td>
</tr>
<tr>
<td>3.10.2</td>
<td>Cybercrime security surveys</td>
<td>103</td>
</tr>
<tr>
<td>3.10.2.1</td>
<td>CSI Computer Crime and Security Survey</td>
<td>103</td>
</tr>
<tr>
<td>3.10.2.2</td>
<td>E-Crime and CyberSecurity Watch Surveys</td>
<td>104</td>
</tr>
<tr>
<td>3.10.2.3</td>
<td>Internet Crime Complaint Centre Surveys</td>
<td>106</td>
</tr>
<tr>
<td>3.10.2.4</td>
<td>Seventh annual e-Crime Congress and KPMG e-Crime survey</td>
<td>106</td>
</tr>
<tr>
<td>3.10.2.5</td>
<td>UK Cybercrime Report 2009</td>
<td>107</td>
</tr>
<tr>
<td>3.10.2.6</td>
<td>South African cybercrime survey</td>
<td>108</td>
</tr>
<tr>
<td>3.10.2.7</td>
<td>Cybercrime surveys conclusion</td>
<td>108</td>
</tr>
<tr>
<td>3.10.3</td>
<td>Understanding the relationship between hackers and cyber criminals</td>
<td>109</td>
</tr>
<tr>
<td>3.11</td>
<td>THE QUESTION OF WHETHER HACKING IS A RISK OR AN EVENT</td>
<td>110</td>
</tr>
<tr>
<td>3.11.1</td>
<td>Introduction</td>
<td>110</td>
</tr>
<tr>
<td>3.11.2</td>
<td>The event component of the term “hacking”</td>
<td>110</td>
</tr>
<tr>
<td>3.11.3</td>
<td>The risk component of the term “hacking”</td>
<td>112</td>
</tr>
<tr>
<td>3.11.3.1</td>
<td>Exploring the different elements of risk</td>
<td>112</td>
</tr>
<tr>
<td>3.11.3.2</td>
<td>Considering risk equations</td>
<td>113</td>
</tr>
<tr>
<td>3.11.4</td>
<td>Conclusion</td>
<td>115</td>
</tr>
<tr>
<td>3.12</td>
<td>THE SIGNIFICANCE OF HACKING IN THE BUSINESS CONTEXT</td>
<td>117</td>
</tr>
<tr>
<td>3.12.1</td>
<td>Introduction</td>
<td>117</td>
</tr>
<tr>
<td>3.12.2</td>
<td>Media coverage of hacking incidents in general</td>
<td>117</td>
</tr>
<tr>
<td>3.12.2.1</td>
<td>Media coverage of hacktivism</td>
<td>118</td>
</tr>
<tr>
<td>3.12.2.2</td>
<td>Media coverage of criminal hacking incidents</td>
<td>119</td>
</tr>
<tr>
<td>3.12.2.3</td>
<td>Media coverage of cyberterrorism</td>
<td>121</td>
</tr>
<tr>
<td>3.12.3</td>
<td>Media coverage of hacking incidents in South Africa</td>
<td>122</td>
</tr>
<tr>
<td>3.12.4</td>
<td>Factors increasing the hacker threat in South Africa</td>
<td>124</td>
</tr>
<tr>
<td>3.12.5</td>
<td>Surveys reflecting on the significance of hacking and cybercrime</td>
<td>125</td>
</tr>
</tbody>
</table>
3.12.5.1 Surveys by PricewaterhouseCoopers 125
3.12.5.2 Survey by Ernst & Young 126
3.12.5.3 Surveys by Deloitte 127
3.12.5.4 Surveys by BERR, Infosecurity and PWC 128
3.12.5.5 Survey by (ISC)² 129
3.12.5.6 Survey by Wolfpack Information Risk (Pty) Ltd. 130
3.12.6 The effect of hacking on an organisation’s reputation 130
3.12.7 Conclusion 131
3.13 FINAL OBSERVATIONS ON THE EFFECTS OF HACKING 132
3.14 CHAPTER SUMMARY 136

CHAPTER 4
HACKING WITHIN THE CONTEXT OF BUSINESS RISK

4.1 INTRODUCTION 139
4.2 DEFINING BUSINESS RISK 140
4.2.1 Business risk viewed from corporate governance codes 141
4.2.2 Diverse views of business risk in literature 142
4.2.3 Business risk views from banking-related sources 143
4.2.4 Identifying common business risks 144
4.3 THE CATEGORIES OR COMPONENTS OF BUSINESS RISK 148
4.3.1 Introduction 148
4.3.2 Physical risk 148
4.3.3 Operational risk 150
4.3.4 Human resource risk 155
4.3.5 Technology risk 158
4.3.5.1 Definition and characteristics of technology risk 159
4.3.5.2 The impact of outdated technology on technology risk 160
4.3.5.3 The impact of new technology on technology risk 161
4.3.5.4 Overlap between the concepts technology risk, systems risk and IT risk 162
4.3.5.5 Technology risk from a corporate governance perspective 164
4.3.5.6 The main focus areas of IT risk prior to the advent of interconnected networks 167
4.3.5.7 New focus areas of IT risks associated with the advent of
interconnected networks

4.3.5.8 Discussion of IT risk from information security sources 170
4.3.5.9 Discussion of IT risk from IT risk management sources 172
4.3.5.10 Discussion of IT risk and control objectives from auditing sources 175
4.3.5.10.1 Views on IT risk from an audit committee perspective 175
4.3.5.10.2 Views on IT risk and control objectives from an internal audit perspective 176
4.3.5.10.3 Views on IT risk and control objectives from an external audit perspective 179
4.3.5.10.4 Conclusion on IT risk and control objectives from auditing literature 183
4.3.5.11 Discussion of internal controls 183
4.3.5.12 Discussion of IT risk from computer and IT auditing sources 186
4.3.5.12.1 Views on IT risk by Davis, Schiller and Wheeler 186
4.3.5.12.2 Views on IT risk by Bezuidenhout 187
4.3.5.12.3 Views on IT risk by Hall 187
4.3.5.12.4 Views on IT risk by Hunton, Bryant and Bagranoff 188
4.3.5.12.5 Views on IT risk by Senft and Gallegos 188
4.3.5.12.6 Views on IT risk by Champlain 189
4.3.5.12.7 Views on IT risk by Pathak 189
4.3.5.12.8 Views on IT risk by Cascarino 190
4.3.5.12.9 Views on IT risk from a leading industry publication and journals 191
4.3.5.12.10 Views on IT risk from conference proceedings 193
4.3.5.12.11 Views on controls from IT auditing sources 193
4.3.5.13 Discussion of IT risk from SAICA standards 194
4.3.5.13.1 Views on IT risk from SAICA’s South African Auditing Standard 195
4.3.5.13.2 Views on IT risk from SAICA Practice Statements 196
4.3.5.13.3 Conclusion on IT risk for SAAS and SAAPS statements 197
4.3.5.13.4 Views on IT risk from International Standards on Auditing and International Auditing Practice Statements 197
4.3.5.13.5 Conclusion on IT risk from ISA and IAPS standards 198
4.3.5.14 Discussion of IT risk from IIA publications 199
4.3.5.14.1 Views on IT risk from IIA’s Practice Advisories 199
4.3.5.14.2 Views on IT risk from IIA’s Global Technology Audit Guides 200
4.3.5.14.3 Views from Guide to the Assessment of IT Risk 203
4.3.5.14.4 Conclusion on IT risk from IIA publications 204
4.3.5.15 Discussion of IT risk from ISACA sources 204
# CHAPTER 5
## THE RESPONSES TO HACKING

5.1 INTRODUCTION 252  
5.2 IDENTIFYING AND CATEGORIZING THE VARIOUS RESPONSES TO HACKING 252  
5.3 HACKING AND THE CORPORATE GOVERNANCE RESPONSE 255  
5.3.1 The essence of the corporate governance response 255  
5.3.2 Application of the corporate governance response 257  
5.3.3 Dimensions of the corporate governance response 258  
5.3.4 Role-players in the corporate governance response 259  
5.3.5 Advantages of the corporate governance response 260  
5.3.6 Disadvantages of the corporate governance response 261  
5.3.7 Risks addressed by the corporate governance response 262  
5.3.8 Conclusion 262  
5.4 HACKING AND THE RISK MANAGEMENT RESPONSE 263  
5.4.1 The essence of the risk management response 263  
5.4.2 The Enterprise Risk Management (ERM) response 265  
5.4.3 Application of the risk management or ERM response 267  
5.4.4 Dimensions of the risk management or ERM response 267  
5.4.5 Role-players in the risk management or ERM response 268  
5.4.6 Advantages of the risk management or ERM response 269  
5.4.7 Disadvantages of the risk management or ERM response 270  
5.4.8 Risks addressed by the risk management or ERM response 271  
5.4.9 Conclusion 271  
5.5 HACKING AND THE INTERNAL CONTROL RESPONSE 273  
5.5.1 The essence of the internal control response 273  
5.5.2 Application of the internal control response 275  
5.5.3 Dimensions of the internal control response 275  
5.5.4 Role-players in the internal control response 275  
5.5.5 Advantages of the internal control response 276  
5.5.6 Disadvantages of the internal control response 276  
5.5.7 Risks addressed by the internal control response 277  
5.5.8 Conclusion 278  
5.6 HACKING AND THE IT GOVERNANCE RESPONSE 278
5.9.1 The essence of the information security management response 294
5.9.2 The information security governance response 295
5.9.3 The security configuration benchmark response 295
5.9.4 The security technology response 296
5.9.5 Application of the information security management response 296
5.9.6 Dimensions of the information security management response 297
5.9.7 Role-players in the information security management response 298
5.9.8 Advantages of the information security management response 299
5.9.9 Disadvantages of the information security management response 300
5.9.10 Risks addressed by the information security management response 301
5.9.11 Conclusion 303

5.10 CHAPTER SUMMARY 304

CHAPTER 6
THE ETHICAL HACKING RESPONSE

6.1 INTRODUCTION 307
6.2 THE ORIGIN AND MEANING OF ETHICAL HACKING AND ETHICAL HACKERS
6.2.1 Introduction 307
6.2.2 Historical origins of the terms “ethical hacking” and “ethical hacker” in brief 308
6.2.3 Defining “ethical hacking” 308
6.2.4 Defining “ethical hackers” 310
6.2.5 Conclusion 312
6.3 ETHICAL HACKER PROFILES 312
6.3.1 Introduction 312
6.3.2 White hat hackers 312
6.3.3 Tiger teams: A synonym for an ethical hacker group 314
6.3.4 Red teaming 314
6.3.5 Conclusion 315
6.4 ETHICAL HACKING METHODOLOGY 316
6.4.1 Introduction 316
6.4.2 Towards a general ethical hacking methodology 316
6.4.3 Preparation phase 320
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.4.4</td>
<td>Footprinting phase</td>
<td>322</td>
</tr>
<tr>
<td>6.4.5</td>
<td>Scanning phase</td>
<td>322</td>
</tr>
<tr>
<td>6.4.6</td>
<td>Enumeration phase</td>
<td>323</td>
</tr>
<tr>
<td>6.4.7</td>
<td>Vulnerability assessment phase</td>
<td>324</td>
</tr>
<tr>
<td>6.4.8</td>
<td>Exploitation phase</td>
<td>324</td>
</tr>
<tr>
<td>6.4.9</td>
<td>Maintenance phase</td>
<td>326</td>
</tr>
<tr>
<td>6.4.10</td>
<td>Recommendation phase</td>
<td>326</td>
</tr>
<tr>
<td>6.4.11</td>
<td>Conclusion</td>
<td>327</td>
</tr>
<tr>
<td>6.5</td>
<td>EXPLORING TERMS SYNONYMOUS WITH ETHICAL HACKING</td>
<td>329</td>
</tr>
<tr>
<td>6.5.1</td>
<td>Vulnerability assessment</td>
<td>329</td>
</tr>
<tr>
<td>6.5.2</td>
<td>Penetration testing</td>
<td>331</td>
</tr>
<tr>
<td>6.5.3</td>
<td>Vulnerability assessment versus penetration testing</td>
<td>334</td>
</tr>
<tr>
<td>6.5.4</td>
<td>Conclusion</td>
<td>336</td>
</tr>
<tr>
<td>6.6</td>
<td>THE PLACEMENT OF ETHICAL HACKERS</td>
<td>337</td>
</tr>
<tr>
<td>6.7</td>
<td>SKILLS REQUIREMENTS AND QUALIFICATIONS FOR ETHICAL HACKERS</td>
<td>341</td>
</tr>
<tr>
<td>6.8</td>
<td>MOTIVATING THE NEED FOR ETHICAL HACKING</td>
<td>343</td>
</tr>
<tr>
<td>6.9</td>
<td>THE APPLICATION OF THE ETHICAL HACKING RESPONSE</td>
<td>345</td>
</tr>
<tr>
<td>6.9.1</td>
<td>Improving information security through ethical hacking</td>
<td>345</td>
</tr>
<tr>
<td>6.9.1.1</td>
<td>Ethical hacking as a complete approach to information security</td>
<td>346</td>
</tr>
<tr>
<td>6.9.1.2</td>
<td>Ethical hacking as part of a larger information security strategy</td>
<td>346</td>
</tr>
<tr>
<td>6.9.1.3</td>
<td>Frameworks that use ethical hacking for improving information security</td>
<td>348</td>
</tr>
<tr>
<td>6.9.2</td>
<td>Using ethical hacking to enhance application security during software development</td>
<td>350</td>
</tr>
<tr>
<td>6.9.2.1</td>
<td>Frameworks that use ethical hacking as part of software development</td>
<td>351</td>
</tr>
<tr>
<td>6.9.3</td>
<td>Ethical hacking as a risk management strategy</td>
<td>352</td>
</tr>
<tr>
<td>6.9.4</td>
<td>Ethical hacking augmenting the effectiveness of other responses to hacking</td>
<td>354</td>
</tr>
<tr>
<td>6.9.4.1</td>
<td>Ethical hacking augmenting the corporate governance response</td>
<td>354</td>
</tr>
<tr>
<td>6.9.4.2</td>
<td>Ethical hacking augmenting the security technologies response</td>
<td>355</td>
</tr>
<tr>
<td>6.9.4.3</td>
<td>Ethical hacking augmenting the baseline security configuration response</td>
<td>355</td>
</tr>
<tr>
<td>6.9.4.4</td>
<td>Conclusion</td>
<td>356</td>
</tr>
<tr>
<td>6.10</td>
<td>THE ADVANTAGES OF ETHICAL HACKING</td>
<td>357</td>
</tr>
</tbody>
</table>
6.11 THE RISKS AND DISADVANTAGES ASSOCIATED WITH ETHICAL HACKING

6.11.1 Risks and disadvantages associated with simulated hacking activity during ethical hacking assignments 360
6.11.2 Risks and disadvantages associated with ethical hacking assignments and the outcome thereof 362
6.11.3 Disadvantages associated with the use of ethical hacking tools 363
6.11.4 Concerns associated with ethical hacking training 364
6.11.5 Conclusion 365

6.12 DIMENSIONS OF THE ETHICAL HACKING RESPONSE 365

6.13 ROLE-PLAYERS IN THE ETHICAL HACKING RESPONSE 366

6.14 ETHICAL HACKING AS A RESPONSE TO BUSINESS RISKS AND IT RISKS 366

6.15 ETHICAL HACKING AND THE LINK WITH CONTROL OBJECTIVES 369

6.16 CHAPTER SUMMARY 370

CHAPTER 7
THE BANKING SECTOR IN SOUTH AFRICA

7.1 INTRODUCTION 374
7.2 SHORT HISTORY AND BACKGROUND OF BANKING IN SOUTH AFRICA 375
7.3 THE DEPENDENCY OF THE BANKING SECTOR ON IT 376
7.4 LOCAL BANKS IN THE SOUTH AFRICAN BANKING SECTOR 379
7.5 ANALYSIS OF THE ANNUAL REPORTS OF THE LOCALLY REGISTERED BANKS 380

7.5.1 Disclosure of corporate governance practices 381
7.5.1.1 Objective of the analysis 381
7.5.1.2 Findings and deductions 381
7.5.2 Disclosure of IT governance practices 382
7.5.2.1 Objective of the analysis 382
7.5.2.2 Findings and deductions 382
7.5.3 Disclosure of business risks 384
7.5.3.1 Objective of the analysis 384
CHAPTER 9
RESEARCH FINDINGS AND RECOMMENDATIONS

9.1 INTRODUCTION 404
9.2 RESEARCH FINDINGS OF THE COMPANY SECRETARY QUESTIONNAIRE 404

9.2.1 Company secretaries’ corporate governance role 404
9.2.1.1 Objective of the question 404
9.2.1.2 Findings and deductions 404
9.2.2 The company secretaries’ views on the board and IT governance 406
9.2.2.1 Objective of the question 406
9.2.2.2 Findings and deductions 406
9.2.3 The company secretaries’ views on IT in business 407
9.2.3.1 Objective of the question 407
9.2.3.2 Findings and deductions 408
9.2.4 The company secretaries’ views on incorporating IT governance into the organisation 409
9.2.4.1 Objective of the question 409
9.2.4.2 Findings and deductions 409
9.2.5 The company secretaries’ views on the individual responsible for IT 410
9.2.5.1 Objective of the question 410
9.2.5.2 Findings and deductions 411
9.2.6 The company secretaries’ views on committees dealing with IT 414
9.2.6.1 Objective of the question 414
9.2.6.2 Findings and deductions 414
9.2.7 The company secretaries’ views on business risk and IT risk 417
9.2.7.1 Objective of the question 417
9.2.7.2 Findings and deductions 417
9.2.8 The company secretaries’ views on hacking and IT risk 418
9.2.8.1 Objective of the question 418
9.2.8.2 Findings and deductions 419
9.2.9 The company secretaries’ views on general responses to hacking 420
9.2.9.1 Objective of the question 420
9.2.9.2 Findings and deductions 420
9.2.10 The company secretaries’ views on the disclosure of IT 423
9.2.10.1 Objective of the question 423
9.2.10.2 Findings and deductions 423
9.2.11 Conclusion 424
9.3 RESEARCH FINDINGS ON THE INDIVIDUAL RESPONSIBLE FOR IT 425
9.3.1 The support that individuals responsible for IT get from their organisation 425
  9.3.1.1 Objective of the question 425
  9.3.1.2 Findings and deductions 425
9.3.2 The views of individuals responsible for IT on the board and IT governance 427
  9.3.2.1 Objective of the question 427
  9.3.2.2 Findings and deductions 427
9.3.3 The views of the individuals responsible for IT on IT in business 429
  9.3.3.1 Objective of the question 429
  9.3.3.2 Findings and deductions 429
9.3.4 The views of the individuals responsible for IT on incorporating IT governance into their organisation 430
  9.3.4.1 Objective of the question 430
  9.3.4.2 Findings and deductions 430
9.3.5 The individuals responsible for IT’s view on business risk and IT risk 432
  9.3.5.1 Objective of the question 432
  9.3.5.2 Findings and deductions 432
9.3.6 The views of the individuals responsible for IT on hacking 433
  9.3.6.1 Objective of the question 433
  9.3.6.2 Findings and deductions 433
9.3.7 The views of the individual responsible for IT on responses to hacking 438
  9.3.7.1 Objective of the question 438
  9.3.7.2 Findings and deductions 438
9.3.8 The views of the individuals responsible for IT on ethical hacking 440
  9.3.8.1 Objective of the question 440
  9.3.8.2 Findings and deductions 440
9.3.9 The experience and qualifications of the individuals responsible for IT 444
  9.3.9.1 Objective of the question 444
## CHAPTER 10
CONCLUSIONS, RECOMMENDATIONS AND AREAS FOR FURTHER RESEARCH

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1</td>
<td>INTRODUCTION</td>
<td>463</td>
</tr>
<tr>
<td>10.2</td>
<td>CONCLUSIONS</td>
<td>463</td>
</tr>
<tr>
<td>10.2.1</td>
<td>Conclusions from the literature study</td>
<td>463</td>
</tr>
<tr>
<td>10.2.2</td>
<td>Conclusions from the analysis of the questionnaires</td>
<td>473</td>
</tr>
<tr>
<td>10.3</td>
<td>RECOMMENDATIONS</td>
<td>477</td>
</tr>
<tr>
<td>10.3.1</td>
<td>Recommendations associated with the meaning of the concept hacking</td>
<td>478</td>
</tr>
<tr>
<td>10.3.2</td>
<td>Recommendations associated with the link between IT risk, business risk and hacking</td>
<td>478</td>
</tr>
<tr>
<td>10.3.3</td>
<td>Recommendations associated with the general responses to hacking</td>
<td>478</td>
</tr>
<tr>
<td>10.3.4</td>
<td>Recommendations associated with the concept ethical hacking</td>
<td>479</td>
</tr>
<tr>
<td>10.3.5</td>
<td>Recommendations associated with the disclosure practices in the local banking sector</td>
<td>481</td>
</tr>
<tr>
<td>10.3.6</td>
<td>Recommendations associated with the responses by the company secretaries and individuals responsible for IT</td>
<td>481</td>
</tr>
<tr>
<td>10.4</td>
<td>AREAS FOR FURTHER RESEARCH</td>
<td>483</td>
</tr>
<tr>
<td>10.5</td>
<td>CONCLUSION</td>
<td>484</td>
</tr>
</tbody>
</table>

REFERENCE LIST

Annexure A: Covering letter to the company secretary
Annexure B: Questionnaire to the company secretary
Annexure C: Covering letter to the individual responsible for IT
Annexure D: Questionnaire to the individual responsible for IT
<table>
<thead>
<tr>
<th>TABLES</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1 King II recommendations on IT</td>
<td>16</td>
</tr>
<tr>
<td>2.2 King III Report principles for the governance of IT</td>
<td>16</td>
</tr>
<tr>
<td>2.3 Examples of IT-related terminology commonly used</td>
<td>26</td>
</tr>
<tr>
<td>3.1 Cybercrime and hacker techniques</td>
<td>98</td>
</tr>
<tr>
<td>3.2 Crimes specifically committed by hackers</td>
<td>102</td>
</tr>
<tr>
<td>3.3 Types of attacks experienced by percentage of respondents</td>
<td>103</td>
</tr>
<tr>
<td>3.4 Types of security technologies used by percentage of respondents</td>
<td>104</td>
</tr>
<tr>
<td>3.5 Crime types as per the CERT 2007 E-Crime Watch Survey, including percentage affected</td>
<td>105</td>
</tr>
<tr>
<td>4.1 Business risk types</td>
<td>143</td>
</tr>
<tr>
<td>4.2 Business risk from an enterprise-wide perspective</td>
<td>143</td>
</tr>
<tr>
<td>4.3 Risks managed by banks on a daily basis</td>
<td>144</td>
</tr>
<tr>
<td>4.4 Comparison of business risk types</td>
<td>145</td>
</tr>
<tr>
<td>4.5 Definition of operational risk components</td>
<td>153</td>
</tr>
<tr>
<td>4.6 Events which could increase people risk</td>
<td>157</td>
</tr>
<tr>
<td>4.7 Technology risk characteristics</td>
<td>160</td>
</tr>
<tr>
<td>4.8 Technology risk factors</td>
<td>160</td>
</tr>
<tr>
<td>4.9 King II recommendations for IT</td>
<td>164</td>
</tr>
<tr>
<td>4.10 King II impact of IT on business</td>
<td>165</td>
</tr>
<tr>
<td>4.11 King II impact of IT on technology</td>
<td>165</td>
</tr>
<tr>
<td>4.12 References to IT risk in the King III Report</td>
<td>165</td>
</tr>
<tr>
<td>4.13 IT risks threatening information security</td>
<td>171</td>
</tr>
<tr>
<td>4.14 IT risk type and risk descriptions considered as part of an information security risk analysis</td>
<td>172</td>
</tr>
<tr>
<td>4.15 Key concepts for the management of IT risk</td>
<td>173</td>
</tr>
<tr>
<td>4.16 IT risk factors</td>
<td>173</td>
</tr>
<tr>
<td>4.17 IT risks relevant to an e-commerce environment</td>
<td>178</td>
</tr>
<tr>
<td>4.18 Information system risks</td>
<td>179</td>
</tr>
<tr>
<td>4.19 Risks associated with business software applications</td>
<td>181</td>
</tr>
<tr>
<td>4.20 Main categories of general controls</td>
<td>182</td>
</tr>
<tr>
<td>4.21 IT risks addressed through general and application controls</td>
<td>182</td>
</tr>
<tr>
<td>4.22 Risks from an e-commerce payment security perspective</td>
<td>187</td>
</tr>
<tr>
<td>4.23 IT risks associated with application systems</td>
<td>189</td>
</tr>
</tbody>
</table>
9.5 The company secretaries’ views on the individuals responsible for IT achieving business objectives
9.6 Job title of the individual responsible for IT
9.7 Reporting line of the individual responsible for IT
9.8 The company secretaries’ views on the individual responsible for IT
9.9 The company secretaries’ views on board committees dealing with IT matters
9.10 The company secretaries’ views on non-board committees dealing with IT matters
9.11 The company secretaries’ views on committees dealing with IT
9.12 Company secretaries’ view on the frequency of IT matters being included in the board of director’s agenda
9.13 The company secretaries’ views of business risk and IT risks
9.14 The company secretaries’ views on hacking increasing various IT risks
9.15 The company secretaries’ views on the extent of general responses to the risk of hacking
9.16 The company secretaries’ views on the effectiveness of general responses to the risk of hacking in their organisation
9.17 The company secretaries’ views on IT disclosure
9.18 The support that individuals responsible for IT get from their organisation
9.19 The views of individuals responsible for IT on the board and IT governance
9.20 The views of individuals responsible for IT on IT in business
9.21 The views of the individuals responsible for IT on incorporating IT governance into their organisation
9.22 The views of the individuals responsible for IT on business risk and IT risk
9.23 The views of the individuals responsible for IT on hacking
9.24 The views of individuals responsible for IT on how hacking increases IT risk
9.25 The views of the individuals responsible for IT on the effectiveness of hacker responses
9.26 The views of the individuals responsible for IT on factors which increases hacking in the banking sector
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.27</td>
<td>The views of the individuals responsible for IT on the responses to hacking in their organisation</td>
<td>438</td>
</tr>
<tr>
<td>9.28</td>
<td>The views of the individuals responsible for IT on the effectiveness of responses to hacking</td>
<td>440</td>
</tr>
<tr>
<td>9.29</td>
<td>The views of the individuals responsible for IT on the effectiveness of ethical hacking as a response in their organisation</td>
<td>441</td>
</tr>
<tr>
<td>9.30</td>
<td>The views of the individual responsible for IT on the use of ethical hacking</td>
<td>441</td>
</tr>
<tr>
<td>9.31</td>
<td>The views of the individuals responsible for IT on the disadvantages of ethical hacking</td>
<td>441</td>
</tr>
<tr>
<td>9.32</td>
<td>The views of the individuals responsible for IT on the advantages of ethical hacking</td>
<td>443</td>
</tr>
<tr>
<td>9.33</td>
<td>The views of the individuals responsible for IT on the use of unique recruitment practices when employing ethical hackers in their organisation</td>
<td>444</td>
</tr>
<tr>
<td>9.34</td>
<td>The highest qualification of the individuals responsible for IT</td>
<td>444</td>
</tr>
<tr>
<td>9.35</td>
<td>The highest IT qualification of the individuals responsible for IT</td>
<td>445</td>
</tr>
<tr>
<td>9.36</td>
<td>Comparative views on the board and IT governance</td>
<td>447</td>
</tr>
<tr>
<td>9.37</td>
<td>Comparative views on IT in business</td>
<td>448</td>
</tr>
<tr>
<td>9.38</td>
<td>Comparative views on incorporating IT governance into the organisation</td>
<td>448</td>
</tr>
<tr>
<td>9.39</td>
<td>Comparative views on the links between business risk and IT risk</td>
<td>449</td>
</tr>
<tr>
<td>9.40</td>
<td>Comparative views on the extent to which hacking will increase and IT risk</td>
<td>450</td>
</tr>
<tr>
<td>9.41</td>
<td>Comparative views on the responses to the risk of hacking</td>
<td>452</td>
</tr>
<tr>
<td>9.42</td>
<td>Comparative views on the effectiveness of the general responses to the risk of hacking</td>
<td>452</td>
</tr>
</tbody>
</table>
## FIGURES

<table>
<thead>
<tr>
<th>FIGURE</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Chapter composition and integration</td>
<td>10</td>
</tr>
<tr>
<td>2.1</td>
<td>A network diagram illustrating the integration of various technologies</td>
<td>24</td>
</tr>
<tr>
<td>3.1</td>
<td>The two dimensions of hackers</td>
<td>51</td>
</tr>
<tr>
<td>3.2</td>
<td>Type of criminal activity categorized in 190 insider attacks</td>
<td>65</td>
</tr>
<tr>
<td>3.3</td>
<td>Hacking as event and risk</td>
<td>116</td>
</tr>
<tr>
<td>4.1</td>
<td>Value chain risk taxonomy</td>
<td>144</td>
</tr>
<tr>
<td>4.2</td>
<td>Two elements of operational risk</td>
<td>152</td>
</tr>
<tr>
<td>4.3</td>
<td>Operational Risk Management (ORM) process view</td>
<td>154</td>
</tr>
<tr>
<td>4.4</td>
<td>IT risk framework</td>
<td>174</td>
</tr>
<tr>
<td>4.5</td>
<td>Positioning IT risk in the organisation</td>
<td>206</td>
</tr>
<tr>
<td>6.1</td>
<td>Comparing ethical hackers with other hacker profiles</td>
<td>313</td>
</tr>
<tr>
<td>6.2</td>
<td>Synonyms for ethical hackers and ethical hacking</td>
<td>315</td>
</tr>
<tr>
<td>9.1</td>
<td>The company secretaries’ views on key drivers towards incorporating IT governance into their organisation</td>
<td>410</td>
</tr>
<tr>
<td>9.2</td>
<td>The views of the individuals responsible for IT on incorporating IT governance into their organisation</td>
<td>431</td>
</tr>
<tr>
<td>9.3</td>
<td>The views of the individuals responsible for IT on factors which increase hacking in the banking sector</td>
<td>437</td>
</tr>
<tr>
<td>9.4</td>
<td>The views of the individuals responsible for IT on the disadvantages of ethical hacking</td>
<td>442</td>
</tr>
<tr>
<td>9.5</td>
<td>The views of the individuals responsible for IT on the advantages associated with ethical hacking</td>
<td>443</td>
</tr>
</tbody>
</table>

## PICTURE

<table>
<thead>
<tr>
<th>PICTURE</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>The UNIVAC I</td>
<td>17</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>AASB</td>
<td>Auditing and Assurance Standards Board</td>
<td></td>
</tr>
<tr>
<td>ACCA</td>
<td>Association of Chartered Certified Accountants</td>
<td></td>
</tr>
<tr>
<td>ACL</td>
<td>Access control list</td>
<td></td>
</tr>
<tr>
<td>ACTA</td>
<td>Anti-Counterfeiting Trade Agreement</td>
<td></td>
</tr>
<tr>
<td>AICPA</td>
<td>American Institute of Certified Public Accountant</td>
<td></td>
</tr>
<tr>
<td>AIRMIC</td>
<td>The Association of Insurance and Risk Managers</td>
<td></td>
</tr>
<tr>
<td>ALARM</td>
<td>The National Forum for Risk Management in the Public Sector</td>
<td></td>
</tr>
<tr>
<td>ARP</td>
<td>Address Resolution Protocol</td>
<td></td>
</tr>
<tr>
<td>B2B</td>
<td>Business-to-business</td>
<td></td>
</tr>
<tr>
<td>B2C</td>
<td>Business-to-commerce</td>
<td></td>
</tr>
<tr>
<td>Basel</td>
<td>Bank for International Settlements</td>
<td></td>
</tr>
<tr>
<td>BBBEE</td>
<td>Broad Based Black Economic Empowerment</td>
<td></td>
</tr>
<tr>
<td>BCM</td>
<td>Business Continuity Management</td>
<td></td>
</tr>
<tr>
<td>BCP</td>
<td>Business Continuity Plans</td>
<td></td>
</tr>
<tr>
<td>BERR</td>
<td>Department for Business Enterprise &amp; Regulatory Reform</td>
<td></td>
</tr>
<tr>
<td>BIOS</td>
<td>Basic input-output system</td>
<td></td>
</tr>
<tr>
<td>BIS</td>
<td>Business Innovation and Skills</td>
<td></td>
</tr>
<tr>
<td>C2C</td>
<td>Consumer-to-consumer</td>
<td></td>
</tr>
<tr>
<td>CEH</td>
<td>Certified Ethical Hacker</td>
<td></td>
</tr>
<tr>
<td>CEO</td>
<td>Chief Executive Officer</td>
<td></td>
</tr>
<tr>
<td>CERT</td>
<td>Computer Emergency Response Team</td>
<td></td>
</tr>
<tr>
<td>CFO</td>
<td>Chief Financial Officer</td>
<td></td>
</tr>
<tr>
<td>CGEIT</td>
<td>Certified in the Governance of Enterprise IT</td>
<td></td>
</tr>
<tr>
<td>CHECK</td>
<td>CESG IT Health Check scheme</td>
<td></td>
</tr>
<tr>
<td>CIA</td>
<td>Central Intelligence Agency</td>
<td></td>
</tr>
<tr>
<td>CICA</td>
<td>Canadian Institute of Chartered Accountants</td>
<td></td>
</tr>
<tr>
<td>CIO</td>
<td>Chief Information Officer</td>
<td></td>
</tr>
<tr>
<td>CIS</td>
<td>Center for Internet Security</td>
<td></td>
</tr>
<tr>
<td>CISO</td>
<td>Chief Information Security Officer</td>
<td></td>
</tr>
<tr>
<td>CISSP</td>
<td>Certified Information Systems Security Professional</td>
<td></td>
</tr>
<tr>
<td>CMMI</td>
<td>Capability Maturity Model Integration</td>
<td></td>
</tr>
<tr>
<td>CobiT</td>
<td>Control Objectives for Information and related Technology</td>
<td></td>
</tr>
<tr>
<td>CoCo</td>
<td>Criteria for control</td>
<td></td>
</tr>
<tr>
<td>COSO</td>
<td>Committee of Sponsoring Organizations of the Treadway Commission</td>
<td></td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
<td></td>
</tr>
<tr>
<td>COO</td>
<td>Chief Operating Officer</td>
<td></td>
</tr>
<tr>
<td>CREST</td>
<td>Council of Registered Ethical Security Testers</td>
<td></td>
</tr>
<tr>
<td>CRO</td>
<td>Chief Risk Officer</td>
<td></td>
</tr>
<tr>
<td>CSE</td>
<td>Communications Security Establishment</td>
<td></td>
</tr>
<tr>
<td>CSO</td>
<td>Chief Security Officer</td>
<td></td>
</tr>
<tr>
<td>CSSA</td>
<td>Chartered Secretaries South Africa</td>
<td></td>
</tr>
<tr>
<td>CVE</td>
<td>Common Vulnerabilities and Exposures</td>
<td></td>
</tr>
<tr>
<td>DBMS</td>
<td>Database management systems</td>
<td></td>
</tr>
<tr>
<td>DDoS</td>
<td>Distributed denial of service</td>
<td></td>
</tr>
<tr>
<td>DEC</td>
<td>Digital Equipment Corporation</td>
<td></td>
</tr>
<tr>
<td>DHS</td>
<td>Department of Homeland</td>
<td></td>
</tr>
<tr>
<td>DISA</td>
<td>Defence Information Systems Agency</td>
<td></td>
</tr>
<tr>
<td>DNS</td>
<td>Domain name system</td>
<td></td>
</tr>
<tr>
<td>DoD</td>
<td>Department of Defence</td>
<td></td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
<td></td>
</tr>
<tr>
<td>DRP</td>
<td>Disaster Recovery Plan</td>
<td></td>
</tr>
<tr>
<td>DTI</td>
<td>Department of Trade and Industry</td>
<td></td>
</tr>
<tr>
<td>e-business</td>
<td>Electronic business</td>
<td></td>
</tr>
<tr>
<td>EC-Council</td>
<td>International Council of E-Commerce Consultants</td>
<td></td>
</tr>
<tr>
<td>e-commerce</td>
<td>Electronic commerce</td>
<td></td>
</tr>
<tr>
<td>EDI</td>
<td>Electronic Data Interchange</td>
<td></td>
</tr>
<tr>
<td>EDP</td>
<td>Electronic data processing</td>
<td></td>
</tr>
<tr>
<td>EDPACS</td>
<td>EDP audit and control and security newsletter</td>
<td></td>
</tr>
<tr>
<td>EFT</td>
<td>Electronic Fund Transfer</td>
<td></td>
</tr>
<tr>
<td>ERM</td>
<td>Enterprise risk management</td>
<td></td>
</tr>
<tr>
<td>ERP</td>
<td>Enterprise resource planning</td>
<td></td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
<td></td>
</tr>
<tr>
<td>EYGM</td>
<td>Limited Ernst &amp; Young Global Limited</td>
<td></td>
</tr>
<tr>
<td>FAIR</td>
<td>Factor Analysis of Information Risk</td>
<td></td>
</tr>
<tr>
<td>FBI</td>
<td>Federal Bureau of Investigation</td>
<td></td>
</tr>
<tr>
<td>FFIEC</td>
<td>Federal Financial Institutions Examination Council</td>
<td></td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
<td></td>
</tr>
<tr>
<td>GCIA</td>
<td>GIAC Certified Intrusion Analyst</td>
<td></td>
</tr>
<tr>
<td>GCIH</td>
<td>GIAC Certified Incident Handler</td>
<td></td>
</tr>
<tr>
<td>GIAC</td>
<td>Global Information Assurance Certifications</td>
<td></td>
</tr>
<tr>
<td>GLBA</td>
<td>Gramm-Leach-Bliley Act</td>
<td></td>
</tr>
<tr>
<td>GPL</td>
<td>General public licence</td>
<td></td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
<td></td>
</tr>
<tr>
<td>GTAG</td>
<td>Global Technology Audit Guides</td>
<td></td>
</tr>
<tr>
<td>HIPAA</td>
<td>Health Insurance Portability and Accountability Act</td>
<td></td>
</tr>
<tr>
<td>HTML</td>
<td>Hypertext Markup Language</td>
<td></td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
<td></td>
</tr>
<tr>
<td>IAASB</td>
<td>International Auditing and Assurance Standards Board</td>
<td></td>
</tr>
<tr>
<td>IAPS</td>
<td>International Auditing Practice Statement</td>
<td></td>
</tr>
<tr>
<td>IBM</td>
<td>International Business Machines Corporation</td>
<td></td>
</tr>
<tr>
<td>iC³</td>
<td>Internet Crime Complaint Centre</td>
<td></td>
</tr>
<tr>
<td>ICSA</td>
<td>Institute of Chartered Secretaries and Administrators</td>
<td></td>
</tr>
<tr>
<td>ICS-CERT</td>
<td>Industrial Control Systems Cyber Emergency Response Team</td>
<td></td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
<td></td>
</tr>
<tr>
<td>IFAC</td>
<td>International Federation of Accountants</td>
<td></td>
</tr>
<tr>
<td>IIA</td>
<td>The Institute of Internal Audit</td>
<td></td>
</tr>
<tr>
<td>IIARF</td>
<td>IIA Research Foundation</td>
<td></td>
</tr>
<tr>
<td>IMF</td>
<td>International Monetary Fund</td>
<td></td>
</tr>
<tr>
<td>IoD</td>
<td>Institute of Directors</td>
<td></td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
<td></td>
</tr>
<tr>
<td>IPS</td>
<td>Intrusion Prevention System</td>
<td></td>
</tr>
<tr>
<td>IRBA</td>
<td>Independent Regulatory Board for Auditors</td>
<td></td>
</tr>
<tr>
<td>IRC</td>
<td>Internet Relay Chat</td>
<td></td>
</tr>
<tr>
<td>IRM</td>
<td>The Institute of Risk Management</td>
<td></td>
</tr>
<tr>
<td>IRMSA</td>
<td>Institute of Risk Management South Africa</td>
<td></td>
</tr>
<tr>
<td>IRM (UK)</td>
<td>Institute of Risk Management United Kingdom</td>
<td></td>
</tr>
<tr>
<td>ISA</td>
<td>International Standards on Auditing</td>
<td></td>
</tr>
<tr>
<td>ISACA</td>
<td>Information System Audit and Control Association</td>
<td></td>
</tr>
<tr>
<td>ISACF</td>
<td>Information Systems Audit and Control Foundation</td>
<td></td>
</tr>
<tr>
<td>(ISC)²</td>
<td>International Information Systems Security Certification Consortium</td>
<td></td>
</tr>
<tr>
<td>ISF</td>
<td>Information Security Forum</td>
<td></td>
</tr>
<tr>
<td>ISG</td>
<td>Information Security Group South Africa</td>
<td></td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
<td></td>
</tr>
<tr>
<td>ISO/IEC</td>
<td>International Organization for Standardization / International Electrotechnical Commission</td>
<td></td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
<td></td>
</tr>
<tr>
<td>ISSA</td>
<td>Information Security for South Africa</td>
<td></td>
</tr>
<tr>
<td>ISSAF</td>
<td>Information System Security Assessment Framework</td>
<td></td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
<td></td>
</tr>
<tr>
<td>ITGI</td>
<td>IT Governance Institute</td>
<td></td>
</tr>
</tbody>
</table>
itSMF  IT Service Management Forum
JSE  Johannesburg Stock Exchange
King II  King Report on Corporate Governance for South Africa 2002
King III Code  King Code of Governance for South Africa 2009
KYC  Know Your Customer
LAN  Local area network
LDAP  Lightweight Directory Access Protocol
LPT  Licensed Penetration Tester
MERIT  Management and Education of the Risk of Insider Threat
MIT  Massachusetts Institute of Technology
MSDL  Microsoft’s Security Development Lifecycle
NASA  National Aeronautics and Space Administration
NATO  Norton Atlantic Treaty Organisation
NFC  Near Field Communication
NIST  National Institute of Standards and Technology
NIST SP 800-30  NIST Special Publication 800-30
NSA  National Security Agency
NVD  National Vulnerability Database
OCTAVE  Operational Critical Threat, Assets, and Vulnerability Evaluation
OECD  Organisation for Economic Co-operation and Development
OSVDB  Open Source Vulnerability Database
OWASP  Open Web Application Security Project
PA  Practice Advisories
PAAB  Public Accountants’ and Auditors’ Board
PASA  Payment Association of South Africa
PC  Personal computer
PCI  Payment Card Industry
PCI-DSS  Payment Card Industry Data Security Standard
PDA  Personal digital assistants
PG  Practice Guides
PIPA  Stop Online Piracy Act
PKI  Public key infrastructure
PMBOK  Project Management Body of Knowledge
PMI  Project Management Institute
PRINCE2  PRojects IN Controlled Environment 2
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PTES</td>
<td>Penetration Testing Execution Standard</td>
</tr>
<tr>
<td>PwC</td>
<td>PricewaterhouseCoopers LLP</td>
</tr>
<tr>
<td>RAS</td>
<td>Remote access servers</td>
</tr>
<tr>
<td>RIMS</td>
<td>Risk and Insurance Management Society</td>
</tr>
<tr>
<td>RMF</td>
<td>Risk Management Framework</td>
</tr>
<tr>
<td>RSA</td>
<td>Republic of South Africa</td>
</tr>
<tr>
<td>SAAS</td>
<td>South African Auditing Standard</td>
</tr>
<tr>
<td>Sabric</td>
<td>South African Banking Risk Information Centre</td>
</tr>
<tr>
<td>SACCI</td>
<td>South African Chamber of Commerce and Industry</td>
</tr>
<tr>
<td>SACFIS</td>
<td>South African Centre for Information Security</td>
</tr>
<tr>
<td>SAICA</td>
<td>South African Institute for Chartered Accountants</td>
</tr>
<tr>
<td>SAMM</td>
<td>Software Assurance Maturity Model</td>
</tr>
<tr>
<td>SANS</td>
<td>SysAdmin Audit Network Security</td>
</tr>
<tr>
<td>SARB</td>
<td>South African Reserve Bank</td>
</tr>
<tr>
<td>SATAN</td>
<td>Security Analysis Tool for Auditing Networks</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory control and data acquisition</td>
</tr>
<tr>
<td>SCAP</td>
<td>Security Content Automation Protocol</td>
</tr>
<tr>
<td>SDL LC</td>
<td>Systems Development Life Cycle</td>
</tr>
<tr>
<td>SensePost</td>
<td>SensePost (Pty) Ltd.</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SOAP</td>
<td>Simple Object Access Protocol</td>
</tr>
<tr>
<td>SOPA</td>
<td>Stop Online Piracy Act</td>
</tr>
<tr>
<td>SOX</td>
<td>Sarbanes-Oxley Act</td>
</tr>
<tr>
<td>SPIT</td>
<td>Spam over Internet Telephony</td>
</tr>
<tr>
<td>SQL</td>
<td>Structured Query Language</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer</td>
</tr>
<tr>
<td>TARA</td>
<td>Threat Agent Risk Assessment</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>Transmission Control Protocol / Internet Protocol</td>
</tr>
<tr>
<td>TOGAF</td>
<td>The Open Group Architecture Framework</td>
</tr>
<tr>
<td>UBANK</td>
<td>UBANK Limited</td>
</tr>
<tr>
<td>UK</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>UN</td>
<td>United Nations</td>
</tr>
<tr>
<td>UPS</td>
<td>Uninterruptible Power Supply</td>
</tr>
<tr>
<td>URL</td>
<td>Universal Resource Locator</td>
</tr>
</tbody>
</table>
US  United States
USA  United States of America
USB  Universal Serial Bus
USSS  US Secret Service
VoIP  Voice over IP
VPN  Virtual private networks
WAN  Wide area network
WEP  Wired Equivalent Privacy
Wolfpack  Wolfpack Information Risk (Pty) Ltd.
XPath  XML Path Language
XSS  Cross-site scripting
CHAPTER 1

Introduction and study layout

1.1 INTRODUCTION

Information technology (hereafter IT) is ingrained in our everyday lives. It enables our social, commercial and financial interaction. More and more financial transactions are taking place across the Internet, both from a personal and organisational perspective, and this introduces the risk of cybercrime, including hacker attacks (Fazekas, 2009:3). The reality of today’s business environment and the dependency on the Internet is described by Grobler (2010b:12) in the following way:

The success of the Internet has not only changed how the world does business, it also has transformed the nature of the risks that organisations face. No longer is it a viable option for organisations to react only once an information security risk emerges. It has become eminent for organisations to know their environments, to anticipate any information security risks beforehand, and to face the cyber impact proactively as part of the organisational strategic plan.

Organisations are critically dependent on IT. Without it, their businesses will not be able to operate. If they do not treat IT as a strategic enabler, organisations will be eliminated by their competitors (Victor & Booysen, 2010:34). This reliance, however, is threatened by numerous IT risks, and, more specifically, hackers. The fact is that organisations are dealing with a threat that is constantly evolving. “Hacking is inherently innovative” (Imperva, 2011:1). This dilemma, and the challenge for organisations in protecting themselves against this threat, is captured in the following quote (Ernst & Young Global Limited, hereafter EYGM Limited 2010:1):

No single technology or process will stop these attacks, and traditional security methods are proving to be ineffective against these threats.

The evolution and advancement of hacking shows a strong alignment with the evolution and advancement in IT. It is a parasitic relationship: hacking cannot occur without IT. With the advancement of technology into the 21st century and the advent of wireless technology and mobile computing devices, hacking as a type of cybercrime has shown similar growth. The explosion of hacking into a multi-million-dollar organised crime world, which is still mostly intangible, largely immeasurable and elusive due to the “underground” nature of criminal
syndicates, is an important concern that must be considered globally (Rodier, 2007:17; Ismail, 2008:13; Protalinski, 2008). Critical system failures due to cyber-attacks and a significant incidence of data fraud and theft are an undeniable reality in today’s global risk landscape (World Economic Forum, 2012:6).

The effect of hacking as an IT risk is further exacerbated by the strong link between IT risk and business risk. This holds true for the banking sector, which relies significantly on technology to enable its business. Cybercrime, which includes the risk of hacking, is regarded as an extremely unpredictable risk (EYGM Limited, 2011). It follows that hacking, as an IT risk, could significantly increase an organisation’s business risks. It is ultimately the board of directors’ responsibility to recognise this.

Organisations sometimes have a false sense of security. The board of directors sometimes assumes that when the organisation has basic security technologies such as firewalls and antivirus software in place, it is secure against hacker attacks. Furthermore, the board may not have the technical knowledge to question the strength or robustness of these security technologies. Operational support to ensure that these security technologies are functional might also be lacking. Or, on the other hand, the likelihood of hacker attacks may be taken for granted, even leading to a lowering of defences. The decentralisation of the workforce and the extended network perimeter pose additional challenges to organisations that want to secure their information assets (Furber, 2011:63-65; Ross, 2011b:4). Insiders (internal hackers) or unauthorised users are the most significant threats to data security (McKendrick, 2011:7). IT risks such as the privacy and security of customer data, protecting intellectual property and compliance with local and international standards and legislation are aspects the board of directors should consider as part of its governance duties. Such factors increasingly require the board of directors to be IT literate (Deloitte Global Services Limited, 2011:1).

Where in the past hackers mostly sought recognition and fame, increasingly today their attacks are aimed at gaining financial reward (Grobler, 2010a:1). Accordingly, the hacker of today, driven by greed, has evolved – often participating in elaborate cybercrime syndicates, stealing confidential data or anything else that exists within the virtual world of organisations and society today (Williams, 2011b):

Indeed, the standard profile of the lone computer hacker has not changed much in 25 years. Brilliant online but often seen as strange in the real world, theirs is an occupation that can be a constructive criminal enterprise or lead to a legitimate fortune.
Numerous high-profile hacker attacks have taken place over the years. During 2011, organisations such as Lockheed, Google, Citigroup, RSA (the security division of EMC) and the International Monetary Fund (hereafter IMF) were attacked (Ross, 2011a:3). Media reports were dominated by attacks perpetrated by the hacker groups LulzSec and Anonymous. The LulzSec hacker group acknowledged that it masterminded several high-profile attacks during the first half of 2011, such as Citigroup, websites of the United States (hereafter US) Senate, the Central Intelligence Agency (hereafter CIA) and the Federal Bureau of Investigation (hereafter FBI) and Sony PlayStation. These attacks mostly consisted of theft of personal user information and credit card details. Losses of up to $1.5 billion have been reported (Solar, 2011). The Sony PlayStation Network was attacked several times during 2011, which led to the service being unavailable to subscribers and significant reputational damage for Sony. A total of 13 Sony websites had been attacked by June 2011, which resulted in various customer data breaches. The personal details of 100 million PlayStation users and losses of up to $13.4 billion have been estimated for the attacks against the Sony PlayStation Network (Paul, 2011; Passeri, 2011; Poulter, 2011; Yasu, 2011:14). Their impact has been described as follows (Chabrow, 2011):

LulzSec is a pest for a growing number of organizations, and their activities have highlighted the unpreparedness of many organizations to safeguard properly their IT assets. And, they've caused some damage and inconvenience, but even more so, embarrassment.

In one of the biggest data breaches of 2011, hackers compromised client details at the email marketing company Epsilon, which provides services to organisations such as Verizon, Citi, Barclay’s Financials, Chase and TiVo. Although the data breach was limited to customer names and email addresses, this attack will most likely increase phishing attacks against these clients (Goldman, 2011; Newman, 2011). Hacker attacks by Anonymous and LulzSec also continued during 2012 (Neal, 2012; Chirgwin, 2012; Muncaster, 2012), the details of which can be found in section 3.12.2.1. These are examples of the unpredictable and damaging nature of hacker attacks, affecting both organisations and the general public alike.

The threat of hacking continues to increase. The Threat Horizon Report for 2013 has highlighted that cybercriminals will become more effective in their use of stolen and publicly available data. Some governments will increase their local hacking capability against cyber-attacks from other opposing governments. Hacktivism will continue to increase and targeted hacker attacks could lead to the complete failure of global information systems (Information Security Forum Limited, hereafter ISF, 2011:16).
Banks are often the target for hacker attacks. Various attack techniques have been designed by hackers and cybercriminals. In recent international attacks, hackers have used a combination of phishing attacks and distributed denial of service (hereafter DDoS) attacks against bank clients. The phishing emails, claiming to be from the National Automated Clearing House Association, were sent to bank clients and DDoS attacks were launched against the banks to block clients from accessing the banks' websites to confirm the validity of the phishing emails (Liebowitz, 2011). In another high-profile attack during May 2011, bank details of 210,000 customers were stolen from Citibank. For this particular attack, it was alleged that a more sophisticated hacker attack technique was used (Kim, 2011; Oates, 2011). Targeted phishing attacks (labelled "spear phishing") have also been used to target the clients of various international banks, such as Citibank, JPMorgan Chase and Barclays (Kitten, 2012). In an alleged insider hacker attack at the South Korean bank National Agricultural Cooperative Federation (known as Non-ghyup), several bank services were affected for a number of days, leaving clients unable to withdraw funds or use credit cards. The internal denial-of-service (hereafter DoS) attack led to the deletion of 5.4 million credit card customer records. A total of 310,000 customers filed a complaint against the bank and 1,000 clients demanded compensation (AFP, 2011:20). Although the banking sector is a significant target for cyber criminals, very little is known about the exact extent of hacker attacks and successful security breaches in this industry. The European Commission might require mandatory disclosure of data breaches via new data protection laws, as there is increasingly more focus on protecting personal details and a greater need for transparency on how the data is secured (Williams, 2011a).

Hacker skills are also utilised as part of cyber warfare. This is a phenomenon on the increase worldwide. The availability of easy-to-use hacker tools and the general increase in bandwidth provisioning across the world increases the impact of these attacks (Ellefson & Von Solms, 2010:2). The attacks against Google, RSA, Lockheed Martin and the IMF were of a cyber-terrorist nature (Kingsley, 2011). Cyber warfare might be initiated by opposing governments, since the sophistication of the attacks requires significant funding (Ross, 2011b:4). During 2011, the British government budgeted £650 million over four years to improve cyber security (Leyden, 2011c). London banks have executed a simulated cyber-attack against 80 participating banks, in preparation for the Olympic Games in 2012, which indicates that cyber warfare is considered a real threat (Leyden, 2011b). Jonathan Evans, Director General of MI5, highlighted during a defence and security lecture that Britain’s National Security Strategy categorises cybercrime at the same level as terrorism. According to him, cybercrime is considered a significant threat to both government and business institutions (Leyden, 2012). Hackers also target oil refineries, and a coordinated attack on
energy installations across the world could lead to a disruption in the global availability of oil and similar commodities (Fineren, 2011). Spy malware, called “Flame”, has been discovered on computers mostly found in Iran. The complex nature of this virus indicates that it was probably a state-funded development, as part of espionage against targeted countries (McElroy & Williams, 2012). This malware also has possible implications for nuclear facilities, similar to the Stuxnet malware found during 2009 (Clayton, 2012). The Department of Homeland (hereafter DHS) Industrial Control Systems Cyber Emergency Response Team (hereafter ICS-CERT) “Incident Response Summary Report” highlighted a significant increase in attacks against industrial controls systems (located in the US) since 2009, pointing out that critical infrastructure could be affected by cyber warfare (ICS-CERT, 2011:2, 13). The increase in Internet bandwidth provisioning in South Africa and strong economic ties with China could place South Africa in the centre of such cyber war attacks (Jansen van Vuuren, Phahlamohlaka & Brazzoli, 2010:1, 8).

The effect of hackers and cybercrime in general also needs to be understood in the South African context. In the absence of collaboration between the private and public sectors to record cybercrime incidents nationally, the overall effect of cybercrime in South Africa remains unknown (Kayle, 2011). Overall, cyber-attacks in South Africa increased during 2011. South Africa currently ranks third in the world in terms of the most phishing attacks. To exacerbate this issue further, only 40% of South African businesses are insured against cybercrime (Maulgue, 2011). The impact of cybercrime in South Africa is bigger than violent crimes (Goredema, 2012). South Africa was also ranked 16th out of the 19 G20 members in terms of its ability to withstand cyber-attacks (Booz Allen Hamilton Inc. 2011:4). The South African ombudsman for banking services awarded R2.16 million to clients who were victims of phishing attacks during 2010 (Mawson, 2011b). South African banking client losses due to phishing attacks reached R180 million in 2010 (Sapa, 2012b). At the start of January 2012, the South African Postbank was attacked by hackers inside the organisation, who misused an employee’s user credentials. Losses of R42 million were reported, and the incident raised questions about the adequacy of Postbank’s security (Rasool, 2012; Styan, 2012). Three people were arrested for the theft early in February 2012. Two have been identified as Post Office employees, with knowledge of the internal systems (Sapa, 2012a).

Against the background sketched above, which illustrates that hacking is a significant threat to organisations, this thesis explores governance responses to hacking. The thesis focuses specifically on how hackers affect the banking sector and assesses whether or not boards of directors are accepting the responsibility of ensuring that an appropriate response has been formulated.
1.2 RESEARCH PROBLEM

Very little research is available internationally and more specifically in South Africa on comprehensive governance responses to hacking. Moreover, no in-depth research has been conducted in the South African banking sector on governance responses to hacking. Therefore, the research problem central to this thesis is to determine what the governance responses to hacking are in the banking sector of South Africa.

1.3 MOTIVATION FOR THE STUDY

As presented in section 1.1, organisations in general are increasingly reliant on IT, due to the pervasive nature of IT in business. This reliance is threatened by a wide variety of IT risks, which are also intrinsically linked to business risk. Hacking is one example of an IT risk that is consistently growing and increasing in sophistication. Boards of directors have the ultimate responsibility of managing and mitigating not only business risk, but also IT risk as part of their IT governance responsibilities. The responsibility of responding to IT risks such as hacking inevitably resides with the board of directors. It therefore needs to be established what the most appropriate response to IT risk and hacking from the board of directors’ perspective is.

The banking sector has a high reliance on technology, which at the same time exposes it to this threat. Given that banks are key drivers of the economy, business and the public at large, it needs to be determined what they are doing in response to IT risk and hacking. It also needs to be determined what lessons can be learnt from the banking sector regarding their current responses to IT risk and hacking.

Linked to this, the board of directors needs to demonstrate its adherence to the principles of King Report of Governance for South Africa 2009 (hereafter King III Report), such as its custodianship of corporate governance, and its responsibility for IT governance and managing risk.

1.4 RESEARCH OBJECTIVES

The overarching objective of this thesis is to explore governance responses to hacking in the banking sector of South Africa. In seeking to achieve this objective, this study will attain the
following outcomes:

- Outline how IT has affected business from a historical perspective, which eventually led to the introduction of IT governance.
- Delve into the meaning and nature of hacking in an effort to understand the significance of this threat in today’s business world.
- Identify common weaknesses found in organisations which facilitate and lead to hacker attacks.
- Provide an overview of the motives and attack techniques of hackers which may lead to security breaches.
- Seek to understand the link between hacking and cybercrime.
- Provide a critical argument for the classification of the nature of hacking as a risk or as an event.
- Identify a common list of business risks to facilitate the discussion of the ultimate link between hacking and business risk.
- Identify common IT risk themes and establish whether a link between hacking and IT risk and control objectives exists, to illustrate that hacking could increase each IT risk theme.
- Identify a link between hacking, IT risk and a range of business risks identified in this study.
- Identify and categorise a range of responses to hacking.
- Explore the depth of each of the responses to hacking, in order to determine whether any of them are effective in addressing all the IT risk themes and by implication the risk of hacking.
- Discuss the origin and meaning of the concept ethical hacking, as well as the associated profiles, methodology, controversial practices and placement of ethical hackers.
- Explore the advantages and disadvantages of, and the motivation for, ethical hacking.
- Explore ethical hacking as a multi-faceted response to hacking.
- Perform exploratory industry-specific research in the banking industry to study governance responses to hacking in the industry.

Complementary to the objectives defined above, as part of the questionnaire fieldwork to be conducted in the local banking sector of South Africa the following primary research objectives have been formulated:

- Given that hackers often target banks, determine what the responses to hacking are in the South African banking sector.
• Determine what the depth of the governance response to hacking is in the banking sector.
• Establish whether the board of directors provides sufficient oversight and focus on IT risk in the local banking sector.
• Determine whether hacking is considered a threat in the local banking sector.
• Determine the extent to which banks make use of ethical hacking as a possible response to the threat of hacking.

In order to achieve these objectives, this thesis will focus on how boards of directors act as a focal point for, and custodian of, corporate governance as they attend to the governance of risk and IT governance.

1.5 BENEFITS AND APPLICATION OF THE STUDY

The key benefit of this study is that it will assist boards of directors in taking responsibility for the governance of risk and for IT governance. Specifically, this study provides a unique in-depth analysis of the link between business risk, IT risk and hacking. In addition, it explores in detail the range of governance responses to hacking. By presenting research results focusing on the banking sector in South Africa and how it deals with the risk of hacking, the study will assist not only the banking industry but business at large in defining appropriate preventative and detective responses to hacking.

1.6 SCOPE OF THE STUDY

This study is located within a South African context, as it focuses on the banking sector of South Africa and the board of directors' responsibilities in the context of the King Code of Governance for South Africa 2009 (hereafter King III Code).

But the principles embodied in the Code and the lessons learnt from the banking sector's responses to hacking may be applied to other sectors and outside the borders of South Africa.

Furthermore, since the primary objective of this study is to identify governance responses to hacking, the focus will be on narrow governance in the South African context. The primary
corporate governance codes that find applicability within this study are the King Report on Corporate Governance for South Africa 2002 (hereafter King II) and King III, which are the prescribed corporate governance codes for all listed companies on the Johannesburg Stock Exchange (hereafter JSE), as set out in the JSE annual report requirements (JSE, 2011:4).

Both King II and King III clearly stipulate that the board of directors carries the ultimate responsibility for governance. This study will reflect this principle in that it focuses on the boards as the primary role-players in the governance arena.

Although the release of King III has reduced the attention paid to King II, this thesis makes extensive use of King II, as its identification of the components of business risk underpins the discussion of the link between business risk, IT risk and hacking. Although King III does not expressly define the components of business risk, it is also a focus point for this thesis due to its inclusion of, and focus on, IT governance.

Excluded from the scope of this thesis are:
- Legislation and regulations addressing hacking. South Africa’s legal framework has been slow in keeping up with advances in technology and related crime, such as hacking, but it has tackled the problem to some extent. However, this thesis is not a legal study. Therefore, only a few general comments related to legislation will be made.
- The technical details of hacking and the technical details of the response to hacking. This thesis focuses on governance response and how the board of directors responds to the risk of hacking, rather than on the technical details.
- Because the study is located in an auditing and governance context, the psychological and cultural aspects of hacking are not given attention here.

Lastly, it must be noted that the scope of cybercrime is wide. The range of computer-related crimes is large and there are simply too many permutations to consider when linking it to business risk. In this thesis, hacking will be singled out as a form of cybercrime and given principal attention.

1.7 LIMITATIONS OF THE STUDY

There is a paucity of comprehensive sources on hacking, governance responses to hacking and ethical hacking. The literature covering these subjects tends to be technical in nature,
elaborating on attack techniques and specific details of software vulnerabilities and exploits. Some of the literature focuses on the psychological or cultural aspects of hackers. Very few sources speak to governance responses to hacking and the board of directors’ responsibilities in this regard. Therefore, non-peer-reviewed literature had to be widely consulted. In so far as statistics and reports on hacker attacks are concerned, the numbers of reports are overwhelming and are available daily. It is therefore not possible to report on all attacks. But suffice it to say that the number, extent and seriousness of hacker attacks are significant.

1.8 STUDY LAYOUT

The study is divided into the following 10 chapters. Graphically the cohesion between some of the chapters can be illustrated, as depicted in Figure 1.1.

Figure 1.1 Chapter composition and integration (own presentation)
1.8.1 Introduction and study layout (Chapter 1)

In this chapter the background to the study, the research problem, objectives, scope and limitations are presented. Chapter 1 also provides an overview of the chapters making up this thesis.

1.8.2 The changing face of IT in business (Chapter 2)

In this chapter a short history of IT and the continued growth and innovation of IT are discussed, to illustrate how integral IT has become as an enabler for business. The chapter also touches on the challenges in managing IT, which calls for proper IT governance in order to ensure that it is fully integrated and aligned with business objectives. The introduction of IT governance highlights the overall significance of IT from a business perspective, emphasising the dependency, accountability and balance required between the derived benefits and risks of IT.

1.8.3 Investigating the meaning and nature of hacking (Chapter 3)

In order to understand the magnitude of the threat of hacking to an organisation, it is important to understand the meaning and nature of the concept. Only then can a proper response be formulated to mitigate the threat in the business world of today. In this chapter the concepts “hacking” and “hackers” are discussed, commencing with the history, evolution of the hacking culture and definitions of the concepts. The profiles, and resulting dimensions and objectives of hackers are explored in order to achieve a better understanding of what motivates their actions and behaviour. Attention is also paid to how they acquire their skills. The chapter goes on to provide a short introduction to hacker methodology, and associated tools and technologies. Weaknesses that lead to successful hacking attacks are also considered, and this is followed by a discussion of hacker attack techniques. Hacking as a type of cybercrime is reflected upon, and this includes an overview of the significance of cybercrime by way of reference to various cybercrime security surveys. This is followed by a critical discussion of whether hacking should be classified as a risk or an event. The chapter concludes with a discussion of the significance of hacking in the business context. This discussion includes reference to media reports and several surveys reflecting the prominence of hacking and cybercrime. This chapter therefore sets the background of the significance of the hacking threat.
1.8.4 Hacking within the context of business risk (Chapter 4)

The significant and pervasive nature of hacking needs to be understood from a business risk perspective. This chapter defines business risk using King II as its foundation, while also considering various other sources, towards the identification of common business risks. Then the chapter provides a discussion of each of the associated business risk types. In particular, technology risk is discussed in detail, also to contextualise IT risk. A comprehensive discussion of IT risk is provided from a number of subject areas and publications relevant to this study. The outcome of this discussion is a list of common IT risks. It is then argued that there is a fundamental link between hacking, IT risk and control objectives. This is followed by a discussion of the links between hacking, IT risk and each of the business risk types, to support the argument of the pervasive nature of hacking across an organisation.

1.8.5 Responses to hacking (Chapter 5)

In order the address the threat of hacking, responses need to be formulated. The chapter commences by identifying broad categories of responses to hacking, which range from the corporate governance response to the information security management response. The chapter goes on to discuss each response in turn, and explores the nature and depth of each response, including the role-players, common best practice framework, advantages and disadvantages and risks addressed by each response. The outcome of this chapter is to assess the effectiveness of each of the responses in addressing IT risk in general and hacking specifically.

1.8.6 The ethical hacking response (Chapter 6)

Chapter 6 focuses on ethical hacking as an alternative governance response to hacking. The chapter provides a discussion of the concepts “ethical hacking” and “ethical hackers” and the skills, qualifications, methodology and training required to conduct ethical hacking. The objectives, motivation, advantages and disadvantages of conducting ethical hacking are also discussed. Emphasis is placed on the use of ethical hacking as a multi-faceted response to business risks, IT risks and hacking. The chapter finally also touches on the controversy associated with ethical hacking, including legal and compliance issues.
1.8.7 Banking in South Africa (Chapter 7)

Chapter 7 commences with a brief overview of the banking sector in the South Africa, as well as the banking sector’s dependency on IT. The chapter then outlines the results of the analysis of the annual reports of the 16 locally registered banks in South Africa. The analysis covers a discussion of the risks and responses identified in this thesis, as disclosed in the annual results of banks. The chapter concludes that the annual reports do not provide enough information to investors and the general public to provide them with insight into how the banking sector manages IT risks, including hacking.

1.8.8 Description of the research methodology (Chapter 8)

Chapter 8 outlines the research methodology followed in this thesis, which consists of a comprehensive literature review, an analysis of the annual reports of the locally registered banks in South Africa and the design and administering of the two research questionnaires in the local banking sector.

1.8.9 Research findings and recommendations (Chapter 9)

The results of the research questionnaires administered in the local banking sector are analysed and discussed and recommendations that can be applied in South Africa and internationally are made.

1.8.10 Conclusions, recommendations and further areas of research (Chapter 10)

This chapter concludes on the overall outcome of the study. Recommendations are presented based on various topics covered in this thesis. Key findings are highlighted and the implications these have for corporate South Africa are discussed.

1.9 THEMATOLOGICAL QUESTIONS

Thematology is the study of themes in literature (Wiktionary, 2012). Thematological questions have been defined throughout this thesis to record common themes discovered in the literature in the form of questions. These questions will be used as the starting point for formulating and distilling pertinent questions required for the research administered via the questionnaires in the local banking sector. Furthermore, the thematological questions can be
used to encourage further research into the topics not covered as part of the research questionnaires.

1.10 CHAPTER SUMMARY

This chapter introduced the study by providing initial background concerning organisations’ critical dependency on IT and the significance of the hacking threat, emphasising that the board of directors is ultimately responsible for ensuring that an appropriate response to the threat of hacking is formulated. The problem statement of the study has been provided, as well as the overall motivation and objectives this thesis sets out to achieve. The scope of the study has also been determined, and this has been followed by an outline of the limitations of this study. The thesis chapter layout has been provided and the purpose behind the use of thematological questions introduced. The next chapter will provide the historical background from which not only IT risk but also the hacking phenomenon emerged.
CHAPTER 2
The changing face of IT in business

2.1 INTRODUCTION

Over the past three decades, the way in which organisations have been governed and controlled has changed dramatically following a spate of corporate collapses and fraudulent financial reporting. The resultant corporate governance codes and legislation that followed are now accepted world-wide as a means of directing and controlling organisations. Corporate governance principles affect all spheres of corporate life and similarly all spheres of corporate life affect corporate governance (Tomasic, 2003:5, 13). However, in the context of this thesis, the impact of IT and a changing IT environment on corporate governance, as well as the effect of corporate governance on the way that IT is approached in a modern business environment, requires further interrogation.

Corporate governance principles have found their way into several pieces of South African legislation, charters and codes: for example, the Protocol on Corporate Governance for State-Owned Enterprises, the Broad Based Black Economic Empowerment (hereafter BBBEE) charters and codes and the Proxy Voting Principles defined by the Public Investment Corporation (Marx, 2008:188, 191-203). Ground-breaking corporate governance codes have been formulated by the Institute of Directors (hereafter IoD) in Southern Africa, the first of which was published in November 1994 (Marx, 2008:178).

The latest authoritative South African corporate governance code, principles and recommendations are set out in the King III Code and the King III Report. General references to both the code and the report will be referred to as King III. King III was preceded by the King II, which still holds considerable value as a corporate governance guideline. Back in 2002, King II already included a list of the areas in which “IT has a significant impact on corporate governance”, being the internal control system, reporting, fiduciary implications, the way business is conducted, technology and the cost value relationship (IoD, 2002:147-150). In making its recommendations, King II also included three important contextual points in Chapter 4 of Section 5 related to IT, which are set out in Table 2.1.
Table 2.1  King II recommendations on IT (IoD, 2002:150)

<table>
<thead>
<tr>
<th>RECOMMENDATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Information technology has had a profound effect on processes within organisations. Accordingly, boards need to ensure that the necessary skills are in place to ensure that their responsibilities in respect of internal control systems are adequately discharged.</td>
</tr>
<tr>
<td>• Potential benefits that result from using technology to improve reporting and transparency should be embraced.</td>
</tr>
<tr>
<td>• Directors need to be mindful of the implications of blurred organisational barriers that arise as a consequence of e-business, to the extent that these result in their governance responsibilities extending beyond the traditional corporate boundaries. They need to ensure that the same levels of governance are applied in the companies with which they integrate along the supply chain.</td>
</tr>
</tbody>
</table>

Whereas King II provided general recommendations regarding IT, King III has taken a significant step forward towards defining very specific principles for the governance of IT. The core guiding principles for the governance of IT are set out in Table 2.2. The King III Report recognises the importance of IT within the business context, as is evident in the following quote (IoD, 2009b:16):

The pervasiveness of IT in business today mandates the governance of IT as a corporate imperative.

Table 2.2  King III Report principles for the governance of IT (IoD, 2009b:82-87)

<table>
<thead>
<tr>
<th>PRINCIPLES</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The board should be responsible for information technology (IT) governance.</td>
</tr>
<tr>
<td>• IT should be aligned with the performance and sustainability objectives of the company.</td>
</tr>
<tr>
<td>• The board should delegate to management the responsibility for the implementation of an IT governance framework.</td>
</tr>
<tr>
<td>• The board should monitor and evaluate significant IT investments and expenditure.</td>
</tr>
<tr>
<td>• IT should form an integral part of the company's risk management.</td>
</tr>
<tr>
<td>• The board should ensure that information assets are managed effectively.</td>
</tr>
<tr>
<td>• A risk committee and audit committee should assist the board in carrying out its IT responsibilities.</td>
</tr>
</tbody>
</table>

It must always be borne in mind that the inherent ongoing complexity associated with IT introduces new risks which should not be underestimated. These risks and the approaches thereto, which will be advocated in this thesis, is explained by Hicks (2001:1):

New cyber-perils that were inconceivable just a few years ago have resulted from computer hacking, viruses and even terrorism. These risks that are inherent in a digital world must be aggressively managed at the highest corporate levels.

Within this context, it is important to reflect on recent history and the remarkable progress
and innovation in IT. Whereas in the past, computer technology was developed reactively as an answer to complex business problems, IT is now pervasive across all spheres of business and has become a predictor of future business trends. Therefore, the purpose of this chapter is to reflect on how technology and IT have evolved in the business environment. In addition, this chapter reflects on the broader developments in IT governance and the importance of IT governance within corporate governance, thus contextualising the risk of hacking within an ever-changing environment.

2.2 REFLECTING ON THE HISTORY OF IT IN BUSINESS PRIOR TO THE 1980s

The first functional computer, the Mark I, was developed by Professor Howard Aiken of Harvard University in 1944. This research was funded by Thomas Watson, the owner of the International Business Machines Corporation, better known today as IBM. The processing power of this computer was comparable to that of a modern-day calculator (Reiss & Dolan, 1989:10; Capron, 1990:652; Computer History Museum, 2006a).

The first computer to attract commercial interest was the UNIVAC I (Picture 2.1), manufactured by Remington Rand in 1951. The UNIVAC I is a typical example of earlier computers, which filled entire rooms with equipment and used magnetic tape as the input and output media.

Picture 2.1 The UNIVAC I (Computer History Museum, 2006a)
During the 1960s, the day-to-day work of both management and staff was affected minimally by the advent of computers. In essence, computers were not interlinked with business processes and were used exclusively for batch processing in order to improve accuracy and efficiency of high-volume transaction processing. Notably, this type of processing was specifically used in the financial services arena (Van Biene-Hershey, 2007:658).

Prior to 1965, most computers could be classified as mainframe computers. In the early part of the 1960s, IBM led the market with their mainframe series, called the System/360 (Capron, 1990:654; Computer History Museum, 2006a). Due to advances in machine architecture, the minicomputer was introduced in 1965, the first being marketed by the Digital Equipment Corporation or DEC (Computer History Museum, 2006c). This development was followed by the advent of microcomputers which made use of powerful microprocessor chips.

Many businesses started using computers in the early 1970s to take advantage of this enhanced processing power, in order to automate repetitive tasks and increase productivity. In 1977, the Commodore PET and Apple II became hugely successful in the home computer market, which in itself created huge business opportunities, and also exposed the general public to computers. Similarly, by that time, minicomputers found widespread use in small and large businesses. Microcomputers introduced productivity software in the form of spreadsheets and word-processing applications into the business arena. Suddenly, microcomputers were no longer simply regarded as toys for hobbyists, but found increased commercial application (Lay, Eccles, Julyan & Boot, 1984:59, 63; Computer History Museum, 2006a). Computers were no longer the domain of the computer specialist, electronic data-processing (hereafter EDP) department and engineers. Staff at various levels in organisations became well versed in using applications in business. Even though management in the late 1970s may not have been completely convinced about the overall returns to the business of IT applications from an investment perspective due to prohibitive costs, the efficiencies in processing did continue to make a huge impact on the way business was conducted (Van Biene-Hershey, 2007:663).

From a technical perspective, over that period, computer technology evolved from using bulky vacuum-tube technology (1951-1958), to transistor technology (1959-1964), followed by integrated circuits (1965-1970). Similarly, data communication technology evolved from the use of modems to transmit data over telephone networks (early 1960s) to the advent of the Internet, through experimental communication technology called the ARPANET, tested by the United States of America (hereafter USA) Department of Defence (hereafter DoD)
and participating universities in the early 1970s, even though the Internet did not have a business application at that time (Lay, et al. 1984:37; Reiss & Dolan, 1989:45; Capron, 1990:654-657; Computer History Museum, 2006b). At least 75% of traffic on the ARPANET consisted of email messages (Peter, 2004).

From an organisational perspective, the application of and control over computers were still largely within the domain of the EDP department. The speed and accuracy of computers were applied to simple processes within the boundaries of the organisation. Management mainly had to concern themselves with the physical security over the data tapes, specifically the theft of data tapes and the consequent loss of mostly financial data were the biggest concern at the time (Van Biene-Hershey, 2007:658-661).

Increasingly from the early 1970s onwards, however, computers also found application in various management and operational tasks. As the exploratory research in this thesis focuses on the banking sector, it is worth noting that at that time computers were widely used in banks (elaborated on in Chapter 7), pension and insurance companies (Watne & Turney, 1990:11-12; Mienes, 2001:40).

2.3 REFLECTING ON THE HISTORY OF IT IN BUSINESS DURING THE 1980s

The 1980s were characterised by a transition from a focus on computers and the efficiencies they could bring, to the field of IT, including advances in communication technologies. In addition, the home computer revolution and its wide application in society as a whole changed the way computer technology was viewed. In the 1980s, accounting systems were designed not only for mainframe systems, but also for mini- and microcomputer systems (Davis, 1996:38). Developments in communication networks introduced local area networks (hereafter LANs), connecting computers at a single site or building and wide area networks (hereafter WANs), linking a number of private networks located at different sites. LANs created local information sharing possibilities with obvious business efficiency advantages, while WANs revolutionised the way in which organisations' distributed locations could communicate and transfer information, thus giving organisations a competitive advantage, allowing them to share information and accelerate business processes (Zwass, 1992:264, 269, 271-272). The use of modems to enable access into an organisation’s network introduced a new risk that organisations were often not even aware of, namely that of unauthorised access, including that by “hackers” (Basta & Halton, 2008:7).
The advent of computer linkages, communication technologies and various forms of networks brought a virtually unstoppable impetus to the advances in the wider field of IT. Control over computer technology was no longer situated within an EDP department or in the accounting function. As IT started having a pervasive impact across organisations, the use of applications grew, whilst an in-depth understanding of complex IT technologies quickly became a specialist function (Capron, 1990:479-491). As a natural consequence, these IT specialists were organised into an IT support function or department, unfortunately often with no direct executive representation (Reiss & Dolan, 1989:423-427).

Due to the growing complexity and diversification of IT, the total number of IT security risks in organisations started to rise. During the early 1980s, businesses were faced with issues regarding privacy of data, confidentiality of data, unauthorised changes to data, availability of IT operations and integrity of IT security measures. IT security departments were introduced to assist management with control over the growing number of IT risks and in response to the need to initiate IT security policies (Van Biene-Hershey, 2007:673).

Further advances in IT during the 1980s enabled the implementation of information systems which provided crucial information to management to assist them in decision making. This led to a further increase in productivity and assisted with strategic planning tasks in the wider organisation. For the first time, management could demand timely, accurate and complete information via IT systems (Lay, et al. 1984:10, 15).

2.4 REFLECTING ON THE HISTORY OF IT IN BUSINESS SINCE THE 1990s AND BEYOND

The need for different organisations to interact with each other introduced Electronic Data Interchange (hereafter EDI) into the business world in the 1990s, which facilitated the electronic exchange of standard business documents (Stone, 1997:28; Pai, 2000:19). From a risk perspective the focus was on errors in processing, corruption of messages, misrouting of transactions and not on the external threat per se (Jenkins, Cooke & Quest, 1992:487).

In the 1990s online systems and electronic commerce became the lifeblood of many organisations. Businesses were opting for 24-hours-a-day operations and IT was required to support this operational demand. Information and the ability to produce information became critical to organisations, so much so that information became an asset and competitive edge for many organisations (Gates, 1999:3). From a cost benefit perspective, Jenkins, et al.
(1992:457) specifically refer to the consistent fall in the cost/performance ratio of computers that characterised the 1990s. This facilitated the pervasive application of IT in the broader business environment.

Looking back at that period, arguably one of the most significant developments in 1991 was the birth of the World Wide Web, as it is known today; its backbone served via the Internet, which makes use of Transmission Control Protocol (hereafter TCP) and Internet Protocol (hereafter IP) to facilitate data transmission. With this development, new concepts were rapidly introduced into the business world. Concepts such as that the World Wide Web consists of multimedia pages, provided via a language called the Hypertext Markup Language (hereafter HTML). A web-browser was required to access these pages, by issuing a Universal Resource Locator (hereafter URL) (for example http://www.uj.ac.za). These became commonplace terms in the business world (Information System Audit and Control Association, hereafter ISACA, 1998:137-138; Kehoe, 2002:1-2, Computer History Museum, 2006b). Stamm (2009:3) highlights that the World Wide Web was not originally designed to be secure. This is also one of the fundamental causes for so many successful hacker attacks, as will be explored in Chapter 3. The Internet, as an alternative to private networks, became a cost-effective means of wider communication for organisations expanding their businesses globally. Virtual private networks (hereafter VPNs) emerged, allowing organisations to share information across the Internet, via secure communication channels (Mapeka, 2000:89; Shue, 2001:20).

After the early 1990s, database technologies matured even further, leading to the development of database management systems (hereafter DBMSs). DBMSs enabled organisations to manage their corporate data as a corporate resource (Bell & Grimson, 1992:14, 16). This necessitated increased integrity and confidentiality of sensitive data, whilst increasing accessibility and processing speed with resultant benefits to organisations.

Other examples of IT technologies which emerged during the 1990s, focusing on the processing and storage of management information, included:

- Enterprise-wide computing.
- Knowledge-based expert support systems.
- Decision support systems.
- Data warehouses and data marts.
- Data mining (Pathak, 2005:2-3).
These technologies further enhanced the support provided to business processes. Increasingly, IT and business processes started to merge. At that time, more and more attention was being paid to the risks associated with those new technologies, specifically in respect of access, which, in light of the emphasis on hacking in this thesis, is obviously important. Consideration was also given to the size and complexity of the organisation, since technologies such as those mentioned by Pathak was not be used in smaller organisations primarily delivering services and goods.

During the 1990s, electronic commerce (hereafter, e-commerce) emerged, which allowed organisations to introduce new IT enabled channels, through which products could be marketed and new business opportunities could be sourced (Kini & Choobineh, 1998:51). An earlier predecessor of e-commerce was EDI, in particular in the retail and automotive sectors (Wagener, 2004:17) where manual ordering processes were replaced by automated ordering systems. Supply-chain management, retail merchandising, brokerages and enterprise resource planning are some of the business areas that benefited significantly from e-commerce (Jutla, Bodorik, Hajnal & Davis, 1999:67). Other than the technologies mentioned earlier by Pathak, e-commerce has the ability to benefit small, medium and large organisations. It has the potential of providing a small organisation an extended network that could expand into international territory (Mapeka, 2000:4; Wagener, 2004:13).

E-commerce is facilitated by network technologies, linking vendors, employees and clients. In the past, organisations had to implement these network technologies themselves or make use of leased lines from their local telecommunication providers. The advent of the Internet and the world wide web during those earlier years has changed this, by significantly bringing down the associated infrastructure cost of e-commerce and also removing geographical boundaries. Making use of the web for e-commerce has to some extent become the most common mechanism to conduct e-commerce activities. The acceptability of conducting business via the Internet has grown to the extent that even electronically signed contracts are considered as legal and binding, similar to their hard-copy counterparts (Wagener, 2004:19). The most prevalent e-commerce types recognised since the 1990s are business-to-business (hereafter B2B) and business-to-customer (hereafter B2C), although other forms are also recognised, such as consumer-to-consumer (hereafter C2C) (Bezuidenhout, 2002:62; Wagener, 2004:22). Different types of goods and services are exchanged via e-commerce (mostly via the Internet). Examples of physical goods include books, CDs, flowers, food, wine and even home appliances. Examples of digital goods include music, computer software and computer games. The Internet also allows companies to differentiate their products from competitors by providing improved services, such as improved
communication and lower costs (Wagener, 2004:24-25). Payment for goods and services can also be facilitated via e-commerce. A typical example is by effecting payment through credit cards. Of course, there are security concerns associated with supplying confidential bank account details (Bezuidenhout, 2002:14; Wagener, 2004:26-27). This is overcome by making use of, for example, encryption, such as enabling Secure Socket Layer (hereafter SSL) on the e-commerce website, which secures the traffic (in this case the bank account details) across the Internet (Mapeka, 2000:112).

During that time, not all organisations or consumers embraced this new concept. There were concerns regarding the security of data flowing across the Internet, issues with the performance of e-commerce sites, cross-border regulatory concerns and a lack of trust from a consumer perspective (Phillips, 1999:59, 61; Kim, 2003:1). Herrera (2009:2) argues that consumers were reluctant to share personal or financial information online. At the root of this mistrust is the fear that criminally-minded individuals such as hackers might intercept or interrupt e-commerce activities (Steube, 2004:6). The significance of the hacker threat will be discussed in detail in Chapter 3.

During the 1990s, a number of new concepts evolved from e-commerce activities. The business areas affected by e-commerce, cumulatively known as electronic business (hereafter e-business), integrating not only internal IT systems, but also those with customers, clients and suppliers effectively using the Internet for e-business communication (Kim, 2003:2; Dilworth & Kochhar, 2004:16; Chuang & Shaw, 2005:3). B2B e-commerce has developed where businesses form an “electronic relationship” between distributors, suppliers and other third-parties to achieve a particular business objective (Chen, 2010:9). Organisations have embraced VPN technology to secure B2B communication across the Internet. VPN technology enables private communication of e-commerce across a public network (Mapeka, 2000:89). B2C e-commerce refers to the engagement between a business and customer via the Internet. Online shopping, enrolling for university courses and online banking are examples of B2C e-commerce interaction (King, 2008:16). Increasingly during that time, physical world commerce was being replaced by virtual world e-commerce.

The late 1990s saw the introduction of enterprise resource planning (hereafter ERP) systems, with organisations such as BAAN, Oracle, PeopleSoft, SAP and J.D. Edwards leading the market. ERP systems made it possible for organisations to integrate production operations with real-time planning, based on customer demand, again giving organisations a competitive edge over their competitors (O’Leary, 2000:27-30). ERP systems facilitated integration of business processes in one single system, by sharing information across the
organisation, thereby improving decision-making processes (Harrison, 2004:16, 19).

In summary, the 1980s and specifically the 1990s were characterised by a new wave of complexity as a consequence of advances in IT and the emergence of layered integrated systems (Parker, 2006:1.29). Different IT technologies had to integrate seamlessly with each other across numerous locations. This is illustrated by the heterogeneous network, connecting various technologies and telecommunications devices, as depicted in Figure 2.1.

Ultimately, as IT became more complex, a detailed understanding and knowledge of IT applications diminished within the wider organisation. Greater levels of specialisation were required to deal with the complex new technologies, for example, sophisticated network equipment, operating systems and programming languages (Van Biene-Hershey, 2007:678). This presented new challenges for boards of directors and management, who are ultimately responsible for all aspects of an organisation.

Figure 2.1  A network diagram illustrating the integration of various technologies (Rate my network diagram, 2007)

Since only those who truly embraced IT were affected directly by these risks, the huge impact of IT on corporate governance was perhaps not that apparent at that time (Van Biene-Hershey, 2007:678).

At the dawn of the 21st century, organisations were slow to adopt information security controls and standards, although professional organisations, for example, ISACA and
external audit firms, highlighted the need for IT governance practices (Gerdes, 2002:28).

2.5 THE PERVERSIVE IMPACT OF IT ON BUSINESS TODAY

The impact of IT on business as an ultimate enabler is more evident today than ever before, when compared to its evolution over the preceding decades. The pace with which IT has evolved has never been more rapid than now. IT no longer finds only limited application in a business environment. IT supports all levels of organisations and all facets of operations, from supply chain management, to direct communication with customers, marketing and selling products beyond the traditional boundaries of organisations, all the way to strategy and decision making at boardroom level.

IT has become an enabler of business strategy and decisions (IoD, 2002:8). The board is responsible for ensuring that the IT strategy integrates with the organisation’s strategy and business processes (IoD, 2009b:83). Management information systems can generate accurate information at the push of a button, and this enables management to make sound decisions on a daily basis. It can empower management to be competitive in an aggressive market, processing millions of transactions in a fraction of the time required to do so manually. Similarly, technology (or more specifically IT) also enables the implementation of controls, including automated controls (Braganza & Franken, 2007:97), significantly increasing efficiency, validity and accuracy of transaction processing (Philee & Philee, 2010:2, 3, 7).

From the turn of the millennium, wireless network technology has become the order of the day (Abdullah, 2006:2). It is now commonplace for employees to work remotely, even from home (Ross, 2006:11), with technologies such as the Internet and wireless network technologies introducing specific business applications. These advances in IT have also led to the personalisation of technology. Cellular telephone technology and personal digital assistants (hereafter PDAs) are opening new business channels for organisations, particularly in the banking industry. In developing countries, where bandwidth costs are still very high and landlines limited (Fourati, 2009:38), cellular technology opens the door for millions of users in underdeveloped areas to gain access to basic services, such as mobile banking services, (Juniper Research Ltd. 2008), leading on to cheaper and easier access to the Internet.

Virtualisation is another key technology that is seeing strong development, providing new
avenues for businesses to manage their IT systems. Virtualisation involves emulating a physical computer on the host server or desktop personal computer (hereafter PC), thereby creating a separate operating system environment (Microsoft, 2009). It facilitates the possibilities forthcoming from cloud computing (scalable and virtualised online resources) and drives the market for software vendors offering their software as a service, particularly online (Beloussov, 2008). Cloud computing vendors provide access to hardware and software as a combined service (Gadia, 2009:24, 27). The organisation effectively outsources all its system needs to a cloud service provider. Access to the cloud service provider is via the Internet. Technology of this kind inevitably introduces new IT risks and vulnerabilities. Whereas cloud computing facilitates easy access to applications and data by third parties and employees alike, it requires protection against fraudsters, selling stolen identities and goods on a “thriving underground online marketplace” (Heske, 2009:25).

The extent to which IT advances have become part of everyday life has also changed the way people communicate with each other in that IT advances have introduced an entirely new set of terminology or jargon into the general business world (some of which is presented in Table 2.3 by way of illustration), and its use has become commonplace today.

### Table 2.3 Examples of IT-related terminology commonly used (own selection)

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>B2E</td>
<td>An “approach in which the focus of business is the employee, rather than the consumer” It is frequently used “to refer to the B2E portal (sometimes called a people portal, which is a customized home page or desk top in organization” (TechTarget, 2010).</td>
</tr>
<tr>
<td>Web 2.0</td>
<td>The “popular term for advanced Internet technology and applications including blogs, wikis, and social bookmarking” (TechTarget, 2008).</td>
</tr>
<tr>
<td>Cookie</td>
<td>“A small text file sent to your computer via your web browser. Cookies store information about you so that a website can remember you; almost like your own identification card. Typical uses include allowing you to log into a website, use a shopping basket and remember your user preferences. Cookies make the interactions between users and websites faster and easier.” Cookies assist organisations in monitoring the habits of the users on the Internet and may be used to profile users for marketing purposes (Premier IT, 2009).</td>
</tr>
<tr>
<td>Phishing</td>
<td>“Form of Internet fraud whereby fake (but legitimate looking) e-mails are used to acquire confidential information such as usernames, passwords and credit card details, in order to steal a user’s identity.” (Premier IT, 2009).</td>
</tr>
<tr>
<td>Shortcut</td>
<td>“A small file containing a target URI (Uniform Resource Identifier) or the name of a target program file that the shortcut represents, making it easier to access from a different location.” (Premier IT, 2009).</td>
</tr>
<tr>
<td>Blogging</td>
<td>“Blogging is the act of posting content on a blog (a Web log or online journal) or posting comments on someone else’s blog.” (Duermyer, 2010).</td>
</tr>
</tbody>
</table>

Looking ahead, the cost of computer technologies will probably continue to decrease, making it more accessible. Enhanced security features are being developed for mobile wireless devices, which brings e-commerce even closer to the end-consumer (R&D Magazine, 2009a; RFinity, 2009). Business transactions will be conducted via virtual personalities. Voice recognition systems, automatic language translation systems, personal security and surveillance systems will become commonplace (Spedding & Rose, 2008:42-
Computing and telecommunication capabilities will become everyday technology in the next decade (Spedding & Rose, 2008:42-43).

Computers will probably become embedded into clothing and become more personalised, with the development of smaller transistors and processors (R&D Magazine, 2009b; Intel Corporation, 2010). Advances in technology will probably move towards the concept of “ubiquitous computing”, where technology is blended with almost everything around us (Greenfield, 2006). This is also referred to as “pervasive computing”, where technology fully integrates with our everyday lives (Sheng, 2010:2). Bartels (2009:1) argues that technology is moving into the “smart computing” phase, which is the next phase in computing history. The smart computing phase was preceded by the “mainframe computing, personal computing and network computing” phases. Smart computing refers to the integration of hardware, software and network technology, including advanced data analytics ability and real world integration, to assist in intelligent decision making to ensure the best business results (Bartels, 2009:3).

Nevertheless, with these advances also come concerns. For example, a 2008 survey conducted by ISACA on the top business issues impacted by technology which may be of specific concern to IT managers and executives highlighted the following issues (ISACA, 2010d:10):

- Regulatory compliance.
- Enterprise-based IT management and IT governance.
- Information security management.
- Disaster recovery/business continuity.
- Challenges of managing IT risks.

Research conducted by the research company Forrester into the state of enterprise IT security for the period 2009 to 2010 has indicated that despite the recent global financial crisis, IT security budgets continued to grow, highlighting the importance of IT security (Penn, 2010:7). The security of data remains a top priority, with fears that IT security is unable to address the increased sophistication of hacker threats. There is growing concern in relation to the security of smartphone and Web 2.0 “social media” technologies, which are growing in popularity and commercial use (Penn, 2010:7). Examples of the application of Web 2.0 are in social community websites, such as Facebook and Twitter. These are increasingly being targeted by attackers, such as hackers and cyber criminals (Mansfield-Devine, 2008:4-5).
Similarly, the American Institute of Certified Public Accountants (hereafter AICPA) identified 10 top technology initiatives for 2010 which were found to be of critical importance to organisations (AICPA, 2010):

- Data security and associated threats.
- Connectivity (wireless and other high speed data lines).
- Business continuity.
- Client portals (to share information between employees, vendors and clients).
- Paperless technology.
- Security of laptops (including encryption).
- Small business software.
- Mobile computing.
- E-filing (such as tax submissions).
- Virtualisation.

When reflecting on these technology initiatives and associated risks, it is clear that the scope of the effect of advances and challenges in IT is very broad. These advances and challenges bring with them IT risks that require a balancing act between the risks and benefits derived therefrom. This relationship between the value or benefits of IT and IT risk is expressed in the opening statement of one of the widely used IT governance models entitled Control Objectives for Information and related Technology (hereafter CobiT) 4.1 (ISACA, 2010a:5):

For many enterprises, information and the technology that supports it represent their most valuable, but often least understood assets. Successful enterprises recognise the benefits of information technology and use it to drive their stakeholders’ value. These enterprises also understand and manage the associated risks, such as increasing regulatory compliance and critical dependence of many business processes on IT.

In the context of this thesis, clearly IT risk must be discussed in detail. This discussion is set out in Chapter 4. However, suffice it to say in this chapter that every organisation should be acutely aware of the risks associated with IT. The extent of this awareness is perhaps best illustrated in the emergence of IT governance globally, particularly from the late 1990s (Political Information, 2009).

<table>
<thead>
<tr>
<th>Thematological research questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Based on the literature review above, the following thematological research questions may be defined:</td>
</tr>
<tr>
<td><strong>Corporate Governance</strong></td>
</tr>
<tr>
<td>The extent to which organisations in the banking sector have direct executive representation on their</td>
</tr>
</tbody>
</table>
board of directors for IT matters.

- Determining where the responsibility for IT security is situated within the banking sector.
- The extent to which the pervasiveness of IT across all spheres of the organisation is reflected in governance and policies and procedures of the banking sector.
- The extent to which new technology is embedded in risk management within the banking sector.

**Business advancement through IT**

- The extent to which IT and business processes have been merged across the banking sector.
- The extent to which information is shared within and outside of the banking sector over the Internet.
- The extent to which IT has made the banking sector more competitive.
- The extent to which the banking sector embraced e-commerce and e-business.
- Top business issues in the banking sector that are impacted by technology.

**IT risks**

- The extent to which the board of directors is familiar with the latest advances in IT and the associated threats emerging in the banking sector.
- The extent to which there is an awareness or focus on the relationship between IT risks and benefits in the banking sector.
- The extent to which the threats associated with e-commerce are known banking sector.

**IT control environment**

- The extent to which a broad range of IT controls has been implemented across the banking sector.
- The extent to which control measures or technological solutions have been considered in securing e-commerce, within the banking sector.

### 2.6 IT GOVERNANCE

Advances in IT have introduced new risks, such as breaches to networks and systems and the loss of confidential information. Organisations started addressing these risks from a corporate governance perspective. This introduced IT governance, as “the link between business and IT” (McGhee, 2008:58). The need for governance in IT has also emerged as a result of increased expenditure on IT, which is not necessarily accompanied by the required return on investment. In addition, ungoverned IT can also have a negative effect on an organisation, as will be explored in this thesis. Whereas in the past the focus might have been on the operational aspects of IT, the focus started shifting to the governance of IT (Standards Australia, 2005:2). In addition, the board of directors might have delegated the decisions regarding IT to the organisation’s IT management or specialist, but with increased regulatory pressure (such as the Sarbanes-Oxley Act, hereafter SOX), the focus on IT risk and the need for a better understanding of IT, the board of directors is required to obtain a deeper understanding of the organisation’s IT and how IT affects the organisation’s strategy (Nolan & McFarlan, 2005:96).
IT governance can be defined as follows:

IT governance can be considered as a framework that supports effective and efficient management of IT resources to facilitate the achievement of a company’s strategic objective (IoD, 2009b:119).

Senior management’s ability to direct, control and evaluate the use of an enterprise’s IT resources in support of the achievement of the organisation’s strategic goals (IT Governance Network, 2009).

A framework for the leadership, organizational structure and business processes, standards and compliance to these standards, which ensure that the organization’s IT supports and enables the achievement of its strategies and objectives (IT Governance, 2009).

IT governance can be viewed from both a micro and macro level. At a micro level, Koo is of the opinion that it refers to “the centralization of IT management to help raise the value of (the) IT department within the organization”. At a macro level, he views it as “a tool to proper corporate governance through the use and application of various IT systems and platforms to help enhance the efficiency and effectiveness of the governance of a company” (Koo, 2007).

Research has shown that the main drivers of the need for IT governance are, firstly, the natural maturing of the IT sector itself (Political Information, 2009) and, secondly, better alignment between business and IT (De Heas & Van Grembergen, 2009:123). A third factor to consider is the need for compliance and control (PricewaterhouseCoopers, 2006:13, 14; Merhout & Havelka, 2008:464). As regards the latter, the regulatory pressures brought about by Bank for International Settlements (hereafter Basel) II in Europe and SOX in the USA requires specific mention. An important requirement of SOX is that management ensures the control and supervision of financial data disclosure, in order to achieve the accuracy, completeness and timeliness thereof. Particularly in organisations that find themselves in multiple locations and across national borders, it is not possible to achieve these goals without robust IT, and therefore IT governance has become critical (Koo, 2007). Effectively, SOX also contributes towards managing risk in organisations (Giniat & Saporito, 2007:66). In the past, operational risk in particular was regarded as a “residual category for risk”. This changed with the introduction of Basel II, which provided specific regulatory guidance for the banking sector towards an operational risk management discipline. Yet again, without effective supporting IT systems, guided by IT governance, operational risk management will
not be successful (Power, 2003:577, 578).

There is an increased focus on the privacy of client data and data security breaches, driven by fears related to the growing sophistication of cybercrime syndicates. Technology countermeasures only are not regarded as effective in curbing these risks. Achieving compliance with regulatory requirements and avoiding reputational risk are foremost in the minds of most organisations. This leads to the “convergence of IT governance, IT risk management and IT compliance”, as a concerted effort to manage IT risks from a governance perspective, across the organisation, whilst firmly establishing accountability for these issues (Dallaway, 2009:12).

Historically, executives and senior management were not intimately familiar with their organisation’s IT governance processes. This often led to significant losses due to poorly managed IT projects. Although there is a growing realisation of the contribution IT makes towards the organisation’s business strategy, there is still a lack of direct accountability over IT and ownership of IT governance. In the South African context this is likely to change with the introduction of King III (IT Governance Institute, 2009a:6, 10; Pedro, 2010:2, 3, 5). Although King II laid the foundation for giving IT its due importance by making boards of directors aware of the significance of e-business and automation of internal control systems within their organisations (IoD, 2002:150), King III takes a significant step towards creating a deeper awareness of the significance of IT at a board of directors’ level (IoD, 2009b:16, 82; Scholtz, 2010:12). The King III Report places emphasis on the strategic nature of IT, the risks forthcoming from IT and the responsibility of the board of directors towards implementing effective IT governance processes (IoD, 2009b:16).

A number of IT governance frameworks and related tools have emerged over the years, some of which also have a more general business application. The most widely used of these are ITIL, Six Sigma, the balanced scorecard, Prince2, CobiT, ISO 17799/ISO 27001, ISO 20 000 (Political Information, 2009) and ISO 27002. The most prominent IT governance frameworks applied today (as opposed to a wider list of IT governance frameworks and tools) will be discussed in detail in Chapter 5. But suffice it for now to note that the need for IT governance has resulted in a number of frameworks and tools to address this need. In general, these IT governance frameworks and tools seek to achieve the same objectives, including (Williams, 2001; Kordel, 2004:40; IoD, 2009b:83, 84):

- Prioritising IT on the board of director’s agenda.
- Alignment of IT objectives with business objectives.
• Reviewing reports of IT's performance.
• Establishing an IT committee as an intermediary between the board and management.
• Ensuring that management follows best practice IT governance frameworks.
• Ensuring that significant IT risks are addressed.
• Ensuring that IT delivers value.

In order to achieve these objectives, it is necessary that IT governance is afforded the appropriate place and importance in each organisation. The importance and state of IT governance is evident in the inclusion of an entire chapter on IT governance in King III, which places the responsibility for IT governance at the highest level in the organisation (IoD, 2009b:31, 82). The wider governance responsibilities toward IT matters by members of the board of directors extend to the fiduciary duties of directors that are closely linked to the changes brought on by technology (Wixley & Everingham, 2005:90). This fiduciary duty is echoed in King II and King III, where the role and function of the board is spelt out in this regard:

The board should … ensure that technology and systems used in the company are adequate to run the business properly and for it to compete through the efficient use of its assets, processes and human resources (IoD, 2002:46).

Companies should understand and manage the risks, benefits and constraints of IT. As a consequence, the board should understand the strategic importance of IT, assume responsibility for the governance of IT and place IT governance on the board agenda (IoD, 2009b:82).

This view is also in line with several proponents of IT governance who argue that accountability for IT governance should be at the highest level in the organisation (Bushell, 2003; Kordel, 2004:39). Looking at the broader picture, this view is also in line with King II, which states that the board of directors has the responsibility of identifying key areas of risk, with specific attention given to technology and systems (IoD, 2002:22). The King III Report has articulated this responsibility even more clearly, by specifically stating that the board is ultimately responsible for IT governance (IoD, 2009b:82). Therefore, advances in technology, and the accompanying risks or threats, of which hacking is the focus area in this thesis, must be considered at the highest levels within organisations. This is because IT has become an integral part of business value. The high investment cost of IT technology and the uncertain nature of IT risks make IT a high-risk area. It is submitted that it is not acceptable for members of the board of directors to “defer” important IT decisions to IT
management. Members of the board need to grasp the fundamental concepts and risks associated with IT (Nolan & McFarlan, 2005:96; Parent & Reich, 2009:138). To manage IT risk, governance in the IT domain has become a necessity (Bloem, van Doorn & Mittal, 2006:3, 11; Rudman, 2008:12). Van Niekerk argues that managing IT risk is a function of IT governance. More specifically, Van Niekerk is of the opinion that an organisation’s information assets should be protected via information security risk management, which can be viewed as a sub-component of risk management (Van Niekerk, 2005:23).

Also of critical importance in the context of this study is Van Niekerk’s view that IT governance cannot be followed or can only be followed to some extent by small, medium and micro-sized organisations (Van Niekerk, 2005:54). This view is relevant to this study, in that the IT risks discussed might only be applicable to some organisations, in particular those that rely significantly on IT. Therefore, it is submitted that the applicability of IT risk is also determined by the size, nature and complexity of the organisation. Similarly, the various responses to IT risk might also only be applicable to some types of organisations. For example, IT risk might be less applicable to a manual-labour manufacturing concern. Hence the focus on the banking sector.

**Thematological research questions**

Based on the literature review above, the following thematological research questions can be defined:

**Corporate Governance**
- The extent to which the board influences the organisation’s information security strategy in the banking sector.

**IT governance**
- The importance afforded to IT governance as a risk-management tool in the banking sector.
- Whether IT governance is seen as part of corporate governance in the banking sector.
- The role that IT governance plays in the banking sector.
- Whether the banking sector applies specific IT governance models.
- Whether there is a clear understanding of IT governance at board level in the banking sector.
- Where the responsibilities for IT governance in the banking sector lie.
- Whether the banking sector’s IT governance is flexible enough to address emerging issues, such as data privacy.
- The extent to which boards of directors have defined their IT governance responsibilities in the banking sector.

**IT risk**
- Whether new e-business ventures increase the banking sector’s IT risk.
- Whether boards of directors focus on IT risk in the banking sector.
2.7 CHAPTER SUMMARY

From the literature study conducted in this chapter, the history of IT and its remarkable and exponential growth in business over the last few decades has been chronicled. Whilst the first available commercial computer, the UNIVAC I in 1951, found only limited application in organisations in general, the 1960s introduced batch-processing activities in business, increasing the application of computers. From the early 1970s, the decreasing cost of computers allowed many organisations to start making use of the enhanced processing power advantages of microcomputers and PCs. Computers were no longer just a research novelty. From the early 1980s, the evolution of IT was not limited to computers, but also found application in network technologies (for example LANs and WANs). This introduced the pervasive nature of IT in business, with the broader application of EDI, e-commerce and database technologies and applications. The Internet was introduced during the 1990s and paved the way for increasingly more sophisticated IT systems, alternative communication paths and wider access to systems. The Internet afforded many organisations the opportunity to start participating in e-commerce and e-business activities.

As explained in this chapter, the increased complexity of IT introduced significant new risks, which require increased attention from boards of directors, who have to be accountable and take responsibility for the risks associated with IT, the extent of which is reflected in the inclusion of IT-related matters in King II and King III (which will be discussed further in Chapter 4) and in the emergence of IT governance. The importance of the board of director’s IT governance responsibilities is clearly evident in the inclusion of and focus on IT governance in King III.

It is therefore clear that IT has evolved and affected business and the risks that are borne in this regard. It is within this context that organisations are faced with a new breed of criminally-minded individuals, who exploit technology to perpetrate “virtual” crimes previously limited to the physical world. These individuals have evolved in congruence with IT, sometimes carrying the label “hackers”. Boards of directors must pay close attention to the threats introduced by hackers in the business environment. Through understanding their nature and motives, a comprehensive response can be formulated to protect the organisation against this threat and by implication fulfil their corporate governance responsibilities.
CHAPTER 3
Investigating the meaning and nature of hacking

3.1 INTRODUCTION

In order to understand the threats posed by hackers, it is essential to understand their motives and actions. After all, a criminal investigation officer sometimes has to put himself in the shoes of the perpetrator to solve a crime. The same principle applies to defining a response to hacking. Chapter 2 of this thesis reflected on how advances in IT have had a profound impact on the way business is conducted and corporations are governed. It is within this context that the primary objective of this thesis is situated: the exploration of the extent to which businesses, with specific reference to organisations listed in the banking sector of the JSE Limited, are addressing the threat of hacking.

Overall, by conducting a comprehensive literature review, the chapter explores the meaning and nature of hacking. Firstly, this chapter will briefly touch on the origins and evolution of hacking, together with definitions for the term “hacking” and “hacker”. This chapter will then go on to focus on the profile of hackers, after which the ways in which they acquire their skills, and their motives and objectives will receive attention. Thirdly, this chapter will pay attention to a common hacker methodology, basic tools and technologies, weaknesses that facilitate successful hacking attempts and hacker techniques, which will later be used in chapter 4 to discuss the link between IT and business risk. Thereafter, hacking as a form of cybercrime is looked at briefly. Lastly, before discussing the significance of hacking in the business context, this chapter will present a case for the classification of the nature of hacking as a risk, on the one hand, and as an event, on the other. This will facilitate the classification of hacking responses as either preventative or detective in nature in chapters 5 and 6.

3.2 THE ORIGINS, EVOLUTION AND MEANING OF HACKING

3.2.1 Introduction

From a historical perspective, the literature shows that the threat of hacking has been prevalent for longer than has perhaps been portrayed in the media. This section will consider
the historical origins and evolution of “hackers” and “hacking”. Thereafter definitions for the terms will be presented to consider the meaning and nature of hacking.

### 3.2.2 Historical origins of the terms “hacker” and “hacking” in brief

The term “hacker” originated in the 1970s, when it was used to refer to individuals who showed a compulsive interest in programming. At that time, memory and storage space were minimal in the first commercially available PCs and therefore software had to be programmed to make use of the limited space. The programmers of the time had to “hack” the software code through repeated application of programming skill and optimisation until it attained a workable small size in order to fit into the limited memory and storage space (Gunkel, 2001:3; Young & Aitel, 2004:32; The Honeynet Project, 2004:507).

During the 1980s, the media started using the term “hacking” to describe individuals who specialise in breaking into computer systems (Macdonald, 2002:347; Denning, 2006).

### 3.2.3 The evolution of hackers and the hacking culture

The literature suggests that the hacking culture can be traced back to 1961, the year in which the Massachusetts Institute of Technology (hereafter MIT) purchased its first PDP-1 (an early minicomputer). It was specifically used by the MIT Tech Model Railroad Club, who invented an entire culture around it. They regarded it as their favourite “tech-toy” and created programming tools and slang or jargon around it (Raymond, 1999; Nissenbaum, 2002:50). These individuals were part of the early highly skilled programmers, called “hackers”. The first password hack was noted in the 1960s when students of MIT used to access the mainframe anonymously. The faculty, however, introduced the use of logon authentication, despite the students’ protest against this. Consequently, the students started guessing the usernames and passwords of other users (Rosenberg, 2000:8). This period of the MIT hackers is referred to as the golden era of hacking. Back then, hacking was purely an intellectual challenge. The literature suggests that when developers of those earlier years started commercialising their software, rather than distributing it for free, the limited number of computer users of that period started having less access to computer software. Another factor was the cost of computer technology, which was generally too expensive for the public and mostly limited to bigger organisations and universities (Rosenberg, 2000:4). Consequently, these early programmers were looking for additional computing resources to allow them to compile their program code. They would hack into labs where computing resources were sitting idle (Schultz, 2002:382). These are seen as the primary reasons for
the criminal element of hacking emerging, since it was believed that access to information and computing resources should be free, a philosophy identified by Levy in his book *Hackers: Heroes of the Computer Revolution*, published in 1984 (Levy, 1984). Arguably, though, the actions taken by those hackers of the time were timid in comparison to the cybercrime activities taking place today (Thomas, 2005:602; Best, 2006:214, 216; Forester & Morrison, 2007:5). Schultz (2002:382) points out that those early hackers followed an unwritten ethical code, which ensured that no damage was caused to systems accessed. In contrast, hackers participating in cybercrime activities today are responsible for significant losses, which will be discussed in section 3.10.

The 1970s introduced a new kind of hacking called “phreaking”, which involved accessing telephone networks and making free calls (Holt, 2005:9-10). John Draper was the first hacker arrested and prosecuted for making long-distance calls without paying for the service (Schell & Martin, 2004:114). Phreaking led to the development of wardialling software in the 1980s, which enabled hackers to discover modems which were connected to organisations’ unprotected systems (Basta & Halton, 2008:7). As computer technology became more accessible during the 1980s, an upsurge in the “computer underground” and hacker activity was noticed (Holt, 2005:10; Thomas, 2005:603).

During the early 1980s, existing legislation in the USA, such as the wire and mail fraud provisions of the federal criminal code, could be used to prosecute some, but not all, cybercrime activities. Due to a growing concern related to the lack of criminal laws to successfully prosecute computer crimes, the United States Congress passed groundbreaking legislation titled “Federal Computer Fraud and Abuse Act of 1986”, which dealt with a wider range of cybercrime activities (US Department of Justice, 2008). A number of high-profile convictions followed, such as the infamous “cult status” hacker Kevin Mitnick’s first arrest in 1988 for breaking into Digital Equipment Company’s computers (Chirillo, 2001:12; Thomas, 2002:197-198; Kabay, 2009:5-6). In the early 1990s, a “great hacker war” ensued between two groups of hackers called Legion of Doom and Masters of Deception. The battle continued for two years, until arrests were made by the FBI in the USA (Chirillo, 2001:12). The late 1990s were characterised by increasingly more sophisticated attacks and a number of hacktivist attacks (to be discussed in section 3.5.3.2). The early 2000s saw the launch of malicious viruses, such as the Lovebug e-mail virus, which crippled many businesses for days (Chirillo, 2001:17, 19). This paved the way for increasingly imaginative criminal activity associated with hackers.

Today, hackers are generally associated with the criminal aspect of the activity of hacking.
Hackers can commit cybercrime through various forms of attack, including DoS attacks, identity theft, web defacements, data theft and fraud. Hackers can affect a system directly through breaking into it, or indirectly by leaving behind Trojan software, which will cause damage at a later point (Stamatellos, 2007:15), all of which will receive attention later in this chapter.

3.2.4 Defining “hackers” and “hacking”

From the information above, it is submitted that the definitions for the terminology “hackers” and “hacking” have different interpretations. These interpretations are also time-bound, in that earlier interpretations were different from those used today.

During the earlier days of computing history, hacking was used to refer to a very skilled programmer. In contrast, it is more recently used to describe security cracking, which involves exploiting vulnerabilities in software and breaking into computer systems (Harris, Harper, Eagle, Ness & Lester, 2005:16; Jordan, 2009). Internet Security Systems (2009) concurs with the idea that hacking has two dimensions. Firstly, in the context of the older meaning, it is said to refer to the hobby or profession of working with computers. Secondly, the more contemporary definition is that it refers to breaking into a computer system. Other writers, such as Thomas (2005:602) and Woo (2003:7-8), also recognise these two dimensions. Similarly, the terminology “hack” and “hacking” refers to the process of using one’s skill in computer programming to gain access to a computer file or network illegally or without authorisation, as well as the act of altering a computer program (thefreedictionary, 2009a).

A “hacker” refers to a person “who is proficient at using or programming a computer, a computer buff” and to a person “who uses programming skills to gain illegal access to a computer network or file” (thefreedictionary, 2009b), again indicating a positive and negative connotation that can be ascribed to hacking. Another interpretation is that a hacker is a “person who writes programs in assembly language or in system-level languages” and that it is a person with a strong technical background (encyclopedia2. thefreedictionary, 2009). Webopedia explains that among professional computer programmers, a hacker can either be a complimentary or derogatory term. However, the latter has become a more common use for the term, while if used as jargon, hacker also refers to a computer enthusiast who “enjoys learning programming languages and computer systems and can often be considered an expert on the subject(s)” (Webopedia, 2003). One of the unique characteristics associated with hackers is their ability of find vulnerabilities in source code.
From a legal perspective, Geissler (2004:163) defined a hacker as “a person that attempts to circumvent the protections of computers from unauthorised access”.

Wysocki (2003:6-8) also supports the views above and argues that hackers have defined the term “cracker”, which will be discussed in the section 3.3.3, to differentiate themselves from the criminal-minded hacker. Nonetheless, Wysocki (2003:10-11) argues that the term “cracker” has not been widely adopted, since “crackers” also label themselves as “hackers”, which has subsequently become common terminology in the media and information security field.

When considering Wysocki’s view, the term hacker takes on a different interpretation from the traditional programming enthusiast. This change in the meaning of the terminology “hackers” and “hacking” needs to be discussed further, in order to reach a common understanding of the terminology.

### 3.2.5 The change in meaning of the words “hacker” and “hacking”

Several writers, such as Skibell (2002:341-342), Taylor (2005:633), Nissenbaum (2004:206) and McHugh and Deek (2005:96), have noted the change in meaning of the terms “hacker” and “hacking”. While at first it referred to the creative and constructive nature of hacking activity, it gradually changed into a more sinister meaning. This shift in meaning of the word “hacking” is captured by Nissenbaum (2004:213):

> Hacking is now imbued with a normative meaning whose core refers to harmful and menacing acts, and as a result it is virtually impossible to speak of, let alone identify, the hackers that engage in activities of significant social value.

Computer crime and hacking activity became known to the public via the media and movies, such as the 1983 movie “WarGames”. The almost mystical ability of hackers to break into computer systems started shaping the “mental image” of the public. Society’s fear for the new computer technology manifested itself in the belief that hackers are evil in nature (Skibell, 2002:341-342). Taylor (2005:633) indicates that the computer security industry specifically vilified hackers, since through an element of fear they created a market place for their security products. The literature therefore suggests that the positive characteristics associated with hacking have been lost in the current meaning of the words “hacking” and “hackers”. Nissenbaum (2004:206) argues that when the FBI started arresting hackers in the 1980s in aggressive hacker “crackdowns”, after the passing of the Computer Fraud and Abuse Act of 1986, sentences issued for hackers were “disproportionately harsh”.

*Chapter 3*
Nissenbaum (2004:206) also argues that journalists started using the terms “hackers” and “hacking” to refer to the “computer vandals”. It is therefore argued that the terms “hacking” and “hacker” carry an overwhelmingly negative connotation, and perhaps it should not be forgotten that there are positive elements associated with hacking, such as the development of open source software and the disclosure of software vulnerabilities to the general computing community.

Despite the above argument, which was true for the period of the 1980s, the hacking culture has evolved alongside technology. Today, the nature of the threat is entirely different and even more significant. This is evident from the motives and objectives of hackers, which will be explored in section 3.5. Hacking’s close link with cybercrime, which will be discussed in section 3.10, poses a significant threat for organisations today.

3.2.6 Conclusion

From the preceding literature review, it is evident that hacking has existed since the 1960s. Traditionally, hackers and hacking have been associated with positive aspects of computing, but nowadays, hacking has taken on a more sinister connotation, as it is associated with illegal activities and with breaking into a computer system in a number of ways and therefore constitutes a threat to organisations. To obtain greater clarity as to the extent of the threat, a literature study on hacker profiles will be conducted.

<table>
<thead>
<tr>
<th>Thematological research questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business risk</td>
</tr>
<tr>
<td>• Whether the board of directors considers the legal implications of hacking in the banking sector.</td>
</tr>
<tr>
<td>Hacker threat</td>
</tr>
<tr>
<td>• The extent to which hackers are regarded as a threat to organisations, particularly in the banking sector.</td>
</tr>
<tr>
<td>• Whether hackers are generally associated with illegal activities and criminal intent, particularly in the banking sector.</td>
</tr>
<tr>
<td>• Whether hacking is seen as a legitimate threat or a general nuisance in the banking sector.</td>
</tr>
<tr>
<td>• The extent to which organisations see hacking as a threat in contrast to other risks the organisation may face in the banking sector.</td>
</tr>
</tbody>
</table>
3.3 HACKER PROFILES

3.3.1 Introduction

To understand hacking as a threat to organisations, it is necessary to consider the wide scope of the profiles of hackers. The media and the motion picture industry typically depict hackers as overconfident, dark and mysterious characters, hacking into systems in a split second (Adam, 2003:3, 4; Thomas, 2002:5-6). Various motion pictures have also popularised hackers, for example WarGames, a well-known film about a hacker who gained access to the USA Defence system, almost accidentally starting a third World War (Thomas, 2002:24; Schell & Martin, 2004:116). The reality is far removed from this stereotype. There are no specific identifiable physical characteristics associated with hackers (The Honeynet Project, 2004:507), yet there are various labels associated with hackers and their activities, with both positive and negative connotations.

The popularisation of terminology defining the stereotypes associated with hacking and hacker profiles is now well established in the literature. The literature suggests that the following commonly defined classes or profiles of hackers can be distinguished (Hafele, 2004:7; Tiller, 2005:27; Skoudis & Liston, 2006:11-13):

- Script kiddies.
- Crackers.
- Über hackers.
- Black hat hackers.
- White hat hackers.
- Grey hat hackers.

In the context of this study, to obtain a clear understanding of each profile and the threat they pose, each of these hacker profiles identified above will be discussed below.

3.3.2 Script kiddies

It is suggested that experienced hackers coined the phrase “script kiddies” for individuals who are novices at hacking (Young & Aitel, 2004:32-33). This term originated in the 1990s, when a sudden increase in new hackers, largely ignoring the original hacker ethic (the principle of free access to all information as discussed in section 3.2.3) and displaying rebelliousness in nature, entered the scene (Thomas, 2005:616). They are also referred to
as “newbies” or “wannabes” (Schell & Martin, 2004:53; Bradbury, 2011:17). When they exclusively use tools to perform their attacks, they are labelled “packet monkeys” (Dion, 2001:2; Henderson & Yarbrough, 2002:12).

Script kiddies collect tools and scripts created by expert hackers (Beaver, 2004:23; Schell & Martin, 2004:53; Bradbury, 2011:17) by contacting other script kiddies or hackers in online chat rooms or via Internet Relay Chat (hereafter IRC). They lack the programming skills of their senior counterparts, hackers (Holt, 2005:85). Script kiddies make up the biggest category of hackers and are a worldwide phenomenon (Skoudis & Liston, 2006:11; Bradbury, 2011:17). They are typically of a younger age, and seek out an easy target, for example a university network. They hack for recreation and to feed their curiosity. They often engage in the act of web-defacement, as a means of displaying their hacker skills level (Liska, 2002:25). Script kiddies will often boast about their successes to friends or fellow hackers and will not see their activities as criminal in nature. They are motivated by the need to be admired as being part of an elite group in the hacker community (Day, 2003:126), speaking to the motives behind their actions. They are regarded as a general nuisance in the information security field (Day, 2003:126).

Research has shown that script kiddies have a limited understanding of the tools and scripts they collect (Tiller, 2005:27; Holt, 2005:7). They will merely execute these tools and scripts randomly, until they find a vulnerable target (Kleen, 2001:2.52). They follow an unstructured approach to hacking. They do not plan their attack, nor do they follow a structured methodology during their attack (Kleen, 2001:3.15). Generally, they do not understand the consequences of their actions (Pearce, 2002:14). They do not know how to cover their tracks or how to break into a specific target. However, their skills level and the amount of damage they are capable of should not be underestimated (Tiller, 2005:27-28; Day, 2003:127). For example, if a script kiddie obtained a zero-day exploit (an exploit not known to the general public), he or she could randomly execute it against numerous targets (organisations connected to the Internet), until he or she successfully manages to break in.

Script kiddies are sometimes driven by sheer determination. The cumulative effect of their efforts could be worsened by launching numerous simultaneous attacks from PCs infected with zombies, the latter referring to any system connected to the Internet which contains a simple vulnerability which will allow the attacker to take control of the computer (Skoudis, 2002:391; Arbor Networks, 2005:2, 9). This could cause a DoS attack due to the high traffic volume created by this simultaneous attack. This could disable the target system or make it very slow to respond to legitimate service requests, preventing authorised users from
accessing the website (The International Council of E-Commerce Consultants, hereafter EC-Council, 2008b:1485-1487). Due to the high volume of scans script kiddies might launch, they could potentially cause significant disruption and financial damage to organisations (Arbor Networks, 2005:9). Script kiddies might also make use of default lists of administrator passwords to access an organisation's IT systems. This is yet again an indication of the novice skill level script kiddies might have. Nonetheless, their success might equal that of their more skilled hacking peers (Macleod, 2007:47).

The literature suggests that recreational or casual hackers may also be categorised as script kiddies. They are individuals who are interested in the mystic lure of hacking and will gain only a limited understanding of hacking (Zager, 2002; Day, 2003:124-125). They could cause more damage than anticipated, for example, by downloading hacker tools which include backdoors that could be used by more skilled hackers to gain entry into a system (Holt, 2005:92, 184). This emphasises the malicious nature of this sometimes benign threat.

As a possible response, organisations can defend themselves against most script kiddie attacks by typical perimeter defence mechanisms, for example firewalls and intrusion detection systems (Day, 2003:127; Henmi, 2006:94).

### Thematological research questions

Based on the literature review above, the following thematological research questions can be defined:

**Hacker profile**
- Whether the banking sector is aware of the term “script kiddies”.
- The extent to which the banking sector comprehends the skills level of script kiddies.
- The extent to which the banking sector can distinguish between script kiddie attacks and hacker attacks.

**Hacker threat**
- The extent to which the banking sector recognises the threat posed by script kiddies.

**Hacking response**
- The extent to which the banking sector has defined defences against script kiddies.

#### 3.3.3 Crackers

As explained in section 3.2.5, nowadays the term hacker is used by the media in general to refer to a criminal perpetrator. However, the literature suggests that historically the term referred to programming enthusiasts (Gunkel, 2001:3). Security specialists and white hat hackers (a category of hacker that will be discussed in section 3.3.6) consequently defined
an alternative term (“cracker”) in 1985, to distinguish between the programming enthusiast and criminally minded individuals (Wysocki, 2003:8; Best, 2003:266; Schell & Martin, 2004:1; Taylor, 2005:628; Leeson, 2006:8). It is suggested that a cracker is a medium-level skilled hacker who might have various ethical reasons for being actively involved in hacking (Young & Aitel, 2004:33). Crackers have a better understanding of the technology, tools and hacker exploits than script kiddies, and will know which tools or exploits to use when targeting a specific organisation or system (Beaver, 2004:23). Crackers will make more effort to collect information about their target objective. They might even use social engineering techniques to obtain information (Arief & Besnard, 2003:3; Frangopoulos, 2007:63). They will be more discreet when they attack a system and will know how to cover their tracks. In order to hide their activities, crackers might use covert channels (hidden within legitimate communication channels) to share tools or download stolen data. The channel provides a level of confidentiality and anonymity (Newman, 2007:1). It is argued that their actions are more focused and specific than those of script kiddies. Consequently, the potential threat level for an organisation is without a doubt higher.

The literature suggests that hackers who make use of password cracking or brute force attacks are often referred to as crackers. This category also includes persons who circumvent or reprogram the software mechanism put in place to protect copyrighted software (Newman, 2006:75; Holt, 2005:180). Crackers will often do more than just break into a system. Once successful in breaking into a system, they will often collect information that could be helpful during later attacks (Arief & Besnard, 2003:2).

Crackers will be aware of the legal ramifications of their actions and they will try to maintain a low profile. In general, they will attack high-profile targets which offer them some sort of reward (for example, a launch pad for further attacks). They will also work hard at obtaining recognition and status in the hacker community (Young & Aitel, 2004:34). Crackers may have pure malicious intent to cause damage to the target system or organisation (Buys & Cronjé, 2004:327; Okenyi & Owens, 2007:303) or to steal data. Crackers may sell their hacking services to criminal individuals or groups (Embar-Seddon, 2002:1037). These actions might be driven through hate or, as mentioned before, simply to gain recognition. Other crackers practise hacking in order to solve a particular problem. This may include changing personal records to erase evidence of misconduct, or simply to show that a particular IT security risk exists in an organisation (Tiller, 2005:29-31).

Although the term cracker was defined to differentiate between programming enthusiasts and criminal hackers, the word “hacker” is also commonly used to refer to “crackers” (Schell
& Martin, 2004:1).

<table>
<thead>
<tr>
<th>Thematological research questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Based on the literature review above, the following thematological research questions can be defined:</td>
</tr>
</tbody>
</table>

**Hacker profile**

- The extent to which the term “cracker” is understood by the banking sector.
- The extent to which “ethical” hacker activities are wrongly associated with criminal cracker activities in the banking sector.
- Whether the term “cracker” is used in the banking sector at all.
- The extent to which a cracker’s skills level and activities are understood by the banking sector.

### 3.3.4 Über hackers

The term “über hacker” (also known as “super” hacker or “elite” hacker) refers to a very small number of exceptionally skilled hackers (Pipkin, 1997:5; Holt, 2005:180). Über hackers have several years of experience and a seemingly unlimited amount of knowledge to ply their trade (Tiller, 2005:31-32). They are exceptional programmers and skilled in the use of operating systems and hardware. They have the skill to disassemble code (reverse engineering software to human readable form) and break encryption patterns (Day, 2003:129). Über hackers write their own tools and exploits, which are often used by other hackers with a lower skills level (Beaver, 2004:23). They have a very high likelihood of success in breaking into any system.

The literature suggests that there is a tendency for über hackers to maintain a low profile and not to publicly share their tools and exploits (Skoudis & Liston, 2006:12; Pipkin, 1997:5). They will plan their attacks carefully, cover their tracks in the process and could cause organisations significant financial losses (Day, 2003:129).

Über hackers will sometimes use sophisticated and complex techniques to break into a system, as opposed to using a simple technique, for example using a brute force password cracking tool. This emphasises their skill, knowledge and pride (Thomas, 2002:71).

It is argued that über hackers are considered to be elite or exceptionally skilled hackers. More recent trends indicate that highly skilled hackers are joining criminal syndicates in order to profit from their criminal activity. These individuals are highly competent and professional, and might infiltrate an organisation by taking on a highly technical position. Rather than writing tools, they could simply buy them. These tactics are to the detriment of
unwary organisations (Zeltser, 2007:34). A similar trend is observed by Pfleeger and Pfleeger (2006:22). Clark (2003:10) points out that it is unlikely that elite hackers will be caught or prevented from hacking into organisations, due to their advanced skills level. This affects the kind of response that has to be defined to mitigate the threat.

<table>
<thead>
<tr>
<th>Thematological research questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Based on the literature review above, the following thematological research questions can be defined:</td>
</tr>
<tr>
<td><strong>Hacker profile</strong></td>
</tr>
<tr>
<td>- The extent to which the banking sector comprehends the skills level of über hackers.</td>
</tr>
<tr>
<td><strong>Hacker threat</strong></td>
</tr>
<tr>
<td>- The extent to which the banking sector comprehends the significance of über hacker activity and the likelihood of success they might have in breaking into a bank.</td>
</tr>
<tr>
<td><strong>Hacking response</strong></td>
</tr>
<tr>
<td>- The extent to which banking sector protects itself against über hackers.</td>
</tr>
<tr>
<td>- How swiftly the banking sector can react to a successful über hacker attack.</td>
</tr>
</tbody>
</table>

3.3.5 **Black hat hackers**

The literature suggests that “black hat” hackers are criminal hackers who act maliciously or with illegal intent (Schell & Martin, 2004:2; Holt, 2005: 158-159, 179). They break into systems in order to use the compromised system as a base to attack other systems, thereby achieving anonymity in the process (Kaminsky, 2006:65). Black hat hackers will steal anything from credit card numbers and trade secrets to confidential client details. They often pursue profit as a main motivation for their actions (Basta & Halton, 2008:3). Depending on the skill and competency of black hat hackers, their actions may lead to unauthorised changes to data, systems and programmes. They could also attempt to process unauthorised transactions, which may lead to errors.

Black hat hackers sometimes join crime syndicates, carrying out extortion or other fraudulent activities (Pashel, 2006:197). The nefarious nature of their activities could lead to irregularities and fraud, branching out to other cybercrime activities. Black hat hackers show contempt for network administrators who do not securely protect their network resources (Arief & Besnard, 2003:11). In some cases they report security concerns to vendors, giving them time to correct the problem. If the vendor does not react in time, the black hat hackers would divulge the information to the general public without considering the consequences. There is also a tendency for black hat hackers to keep the information secret and use it only
for their own personal gain (Young & Aitel, 2004:35).

Importantly, it must also be noted that more recently underground black hat communities have started to form. One of the techniques used to sell their newly developed exploits is to host auction sites on the Internet. In general, it has become easier to enter the black hat community. Black hat hackers were traditionally distinguished as having excellent programming skills. However, today, fully functional automated exploit software is available for purchase by any aspirant black hat hacker (Holt, 2005:158-159; Bloor, 2007). This clearly demonstrates how motive could carry more weight than skills level, since the automation of hacking accelerates the skills level of the hacker and in some cases negate the need for high skills levels.

### Thematological research questions

Based on the literature review above, the following thematological research questions can be defined:

#### Hacker profile
- Whether the banking sector have the ability to distinguish black hat hackers from white or grey hat hackers, according to the malicious nature of the attacks.

#### Hacker threat
- Whether the banking sector can detect black hat hacker activity on their network and systems.
- Whether there is an awareness of the type of exploits undertaken by the underground black hat community and the potential impact these exploits might have on banks.
- The extent to which there is awareness that black hat hackers could potentially buy all the hacking tools and exploits required to break into a bank, which possibly increases the likelihood of success.

### 3.3.6 White hat hackers

It is suggested that “white hat” hackers do not have the same sinister intentions “black hat” hackers may have. They are seen as the “good guys” in the computer underground (Schell & Martin, 2004:2; Thomas, 2005:601, 617; EC-Council, 2008a:28). They have an interest in computer security and may seek out vulnerabilities in computer systems in order to warn the general public (Young & Aitel, 2004:34; Parker, Devost, Sachs, Shaw & Stroz, 2004:226). White hat hackers will not break into a system if they do not have sufficient authorisation to do so. Alternatively, they may break into a system without causing any damage (Leeson, 2006:10).

White hat hackers frequently develop tools to help prevent attacks by other hackers. White hat hackers often work in the information security field (EC-Council, 2008a:30) and have
often completed some form of formal training, such as an undergraduate degree in computer science. They are also called “sneakers” or “white knights” on occasion (Benish, Cheifetz, Darche, Reed & Uhls, 2005; Vernersson, 2010:7).

The defining difference between white hat and black hat hackers is that white hat hackers adopt an ethical viewpoint. Consequently, white hat hackers are often classified as “ethical hackers” (Holt, 2005:7; EC-Council, 2008a:30). Duke (2002:3) warns, however, that white hat hackers sometimes seek public exposure to “satisfy their own inflated egos” and may act suspiciously.

White hat hackers are in general considered to be skilled hackers, often working in the information security field or as independent information security consultants, as Holt (2005:94) argues. In contrast, however, Hancock (1999:285) warns that white hat hackers could be inexperienced. Hancock further argues that when they are employed by a security organisation, the organisation will not disclose the particular details of previous assignments, since it may be confidential in nature. He also goes on to point out that white hat hackers may lack information security qualifications. White hat hackers may therefore have a varying degree of skill, experience and qualifications, although it would generally be assumed that they have at least an intermediary skills level.

As to the effect of performing hacking activities on an organisation, it is submitted that generally a white hat hacker’s activity would have no adverse effect on an organisation (depending of course on the individual’s skills level and the care he or she takes in his or her conduct). However, even though theoretically white hat hackers will hack into a target only with the target’s permission (which involves standby procedures to ensure that there is no disruption to business processes), risks still exist in relation to the activities of white hat hackers (Kaminsky, 2006:64). On the one hand this risk could lie in any degree of business interruption that may result from their activities, while on the other hand, there is the risk that the white hat hacker could decide to apply his trade in a more sinister way at any time (Duke, 2002:3). White hat hackers also have to be cautious that their activities are not regarded as irregular or illegal (Luoma & Luoma, 2009:99) and they will have to consult laws applicable to every country in which they operate, as well as the policies and procedures of their targets, to determine the boundaries within which they can operate.
Based on the literature review above, the following thematological research questions can be defined:

**Hacker profiles**
- The extent to which the banking sector clearly comprehends the objectives of white hat hackers.
- Whether the banking sector is cautious in appointing white hat hackers.
- The extent to which there is an understanding that white hat hacker activities will in general not have an adverse effect on banks and their systems.
- Whether the banking sector realises that a white hat hacker’s motives could be unclear.

**Ethical hacking**
- The extent to which the banking sector can manage white hat assignments to ensure minimal business disruption.

### 3.3.7 Grey hat hacker

“Grey hat” hackers are regarded as a hybrid of white hat and black hat hackers (Poulsen, 2000; The Honeynet Project, 2004:508). Grey hat hackers would potentially break into an organisation, without causing any damage. Their motive is to provide proof that it is possible to break into a particular organisation. Whether grey hat hacker actions are ethical and whether they have respect for the affected victim are questionable, though (Piscitello, 2005b). The literature suggests that grey hat hackers are seen as fence-sitters; the wolf in sheep’s clothing who will release exploits to the vendor and to the public (Holt, 2005:7). They believe in full disclosure of vulnerabilities within systems, without considering the consequences of the disclosure (Lee, 2002:39; Lemos, 2002a). Therefore, on the one hand they may work as security professionals, but on the other hand they may leak vulnerabilities to the hacker community, including to black hat hackers.

At times, grey hat hackers may falsely label themselves as white hat hackers. One such an example is Max Butler, a self-proclaimed white hat hacker, who was prosecuted in the USA for breaking into several organisations, such as the National Aeronautics and Space Administration (hereafter NASA). Butler was the author of an open source attack signature database, arachNIDS, which has been used to detect hacker attacks. He also provided advice to the FBI on computer crime cases. Despite these “white hat hacker” activities, he broke into the McCord Air Force Base and NASA’s Marshall Space Flight Center, among other organisations (Poulsen, 2000). A second example is another self-proclaimed white hat hacker, Kevin Finisterre, employed by Secure Network Operations, who disclosed one of the vulnerabilities discovered on an assignment conducted at HP. HP threatened the organisation with litigation under the Digital Millennium Copyright Act, after Finisterre...
disclosed one of the vulnerabilities and how it can be exploited to the general public (Lemos, 2002b).

Hacktivist groups (which will be discussed in section 3.5.3.2) can be classified as grey hat hackers, since they may deface an organisation’s website as a message of activism (Basta & Halton, 2008:3). Grey hat hacker activity, such as the activity of the LulzSec hacker group, is at times welcomed, as it highlights security vulnerabilities in a number of organisations (Raywood, 2011).

Thematological research questions

Based on the literature review above, the following thematological research questions can be defined:

**Hacker profiles**
- Whether the banking sector understands the concept grey hat hacking and how it differs from either white hat or black hat hacking.
- Whether the banking sector can differentiate between white hat hackers and grey hat hackers when either hiring hackers or appointing a security firm to conduct ethical hacking assignments.

**Hacker threat**
- Whether the banking sector can identify and protect itself against grey hat hacker activity.

3.3.8 The resultant two dimensions of hackers

From the discussion presented in this thesis, it is clear that two dimensions of the profile of hackers come to the fore. The first is related to the skills level of hackers, which ranges from novice to seasoned experienced individuals. The second is related to the purpose of their actions, or, put otherwise, the ethical goal-oriented viewpoint of hackers that ranges from moral or ethical to immoral or unethical behaviour. It is therefore possible to define a method of classifying hackers according to their skills level and ethical viewpoint.

Firstly, considering the skills levels of hackers discussed in this thesis, clearly one should distinguish between script kiddies, crackers and über hackers. This classification is supported in the literature by writers such as Pipkin (1997:3), Loper (2000:21), Voiskounsky and Smyslova (2003:172), Hafele (2004:7), Tiller (2005:27), Skoudis and Liston (2006:11-13) and Hall and Singleton (2005:226).

Secondly, considering the ethical viewpoint of hackers discussed in this thesis, three categories of hackers can be distinguished: the black hat hacker, the white hat hacker and the grey hat hacker. It is claimed that the analogy comes from old Western movies, where the “good guy” wore a white hat and the villain a dusty black hat. This classification is

In support of this classification method, Holt (2005:6-7) argues that hackers often classify themselves as white, grey or black hat hackers. Barber (2001:17) is of the opinion that over time hackers may swap between the various ethical viewpoints, such as an adolescent who may initially be involved in black hat hacker activity and later change to a white hat hacker, when faced with adult responsibilities. Barber (2001:17) points out that hackers often make a conscious decision at some point in their lives as to the ethical viewpoint they wish to follow.

When considering both the skills level of hackers and ethical viewpoint as presented above, it is possible to view them as two dimensions which can be used to classify hackers (own deduction). The two dimensions of hackers are depicted in Figure 3.1 below. The positions of the hacker profiles on the graph are relative and not definitive, however Figure 3.1 display the typical position of the hacker profiles (own deduction).

**Figure 3.1** The two dimensions of hackers (own interpretation)

![Diagram of hacker dimensions](chart.png)

The two dimensions also work interchangeably, in that hackers with a certain skills level could have a specific ethical viewpoint and vice versa. For example, a white hat hacker could have a script kiddie skills level (own deduction).
Hacker profiles

- Whether the banking sector realises that there are both a skills level and ethical viewpoint associated with hackers, which work interchangeably.
- Whether the two dimensions of hackers can be applied by the banking sector to help them in identifying the most significant threat.

3.3.9 Conclusion

A number of different profiles of hackers have developed over time. The analysis of these profiles shows a clear focus on either the skills levels of hackers or on their motives or ethical viewpoints. As the threat that hackers holds for any organisation will vary depending on their skills level and ethical viewpoint, it is important to focus further on each of these two areas.

Henceforth in this thesis, hackers and hacking will generally refer to people performing the illegal activity of breaking into a system or network to pursue fraud or steal data, thereby intentionally or unintentionally causing damage to an organisation’s tangible or intangible assets. Detective and preventative responses will be defined for this perpetrator. Where appropriate, the specific hacker profile will be used to provide greater clarity.
Even though nowadays hacking is associated with criminality, there are a number of widely accessible sources that hackers and ethical hackers may use to acquire their skills that are in themselves not associated with a criminal act. These range from the Internet itself, to freely available source codes, to books on the subject.

The best place to acquire the trade secrets of hackers is also the medium that contributes significantly to the success of hacking: the Internet. Hacking tools and how-to guides are freely available from the Internet (Pipkin, 1997:17; Woo, 2003:15). Good examples of white hat hacker websites listing or hosting hacking tools (classified as security tools) include Lyon (2011) and The Hacker’s Choice (2008). This is also the starting point for script kiddies, who visit publicly accessible websites, such as online chat forums, and follow the guidance provided by more experienced hackers and ethical hackers (Schell & Martin, 2004:53; Holt, 2005:73). The availability of automated hacker tools has also made it easier for an aspiring hacker to start engaging in this activity (Yar, 2006:32). It is even possible to download preconfigured CDs with numerous tools already installed and ready to use. An example of such a CD is BackTrack, published as an ethical hacker toolkit (remote-exploit.org, 2007), but that could obviously also be applied by hackers with a more sinister motive.

The literature suggests that hackers also frequently use IRC to communicate with other hackers (Loper, 2000:31). IRC is also used to exchange exploits and hacker techniques. Often hackers will compromise servers and use them as platforms to establish secret IRC services (Arief & Besnard, 2003:13). Through anonymous chat lines, hackers share hard-to-find exploits and tips with fellow hackers.

It is also suggested that hackers have founded groups or “gangs” in order to share their knowledge and skills. One of the first hacker gangs, called “414”, gained access to the computer system at the Los Alamos National Laboratory, where nuclear weapons were developed (Leeson, 2006:5). Other examples of well-known hacker groups include The Cow of the Dead Cult (cDc Communications, 2007), popular for its hacktivist activities and the release of its Trojan tool called Back Orifice (Thomas, 2002:89) and The Hacker’s Choice (2008), a group that produces many tools used within the hacker and ethical hacker community.

Security conferences, such as the annual BlackHat and DefCon conference hosted in Las Vegas, are also a possible source of information for hackers and ethical hackers. Even
information security conferences, such as ITWeb hosted in South Africa, provide some insight into known and emerging software vulnerabilities and hacker techniques (ITWeb Limited, 2009).

Finally, in recent years, quite a number of books have been written on the subject of hacking. Although mostly aimed at the information security field, these books could be used by novice hackers to enhance their skill in the techniques of hackers. In themselves, the books raise some controversy, as they may assist in perpetuating hacker activity. One of the solutions to this controversy seems to be for authors to always include and describe countermeasures, when showing how vulnerabilities could be exploited (Harris, et al. 2005:12).

<table>
<thead>
<tr>
<th>Thematological research questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Based on the literature review above, the following thematological research questions can be defined:</td>
</tr>
</tbody>
</table>

**Hacker threats**
- The extent to which there is awareness in the banking sector that hacker tools and how-to guides are freely available on the Internet.
- The extent to which there is a realisation in the banking sector that several books have been written on the topic of hacking and related attack techniques.
- The extent to which there is a realisation in the banking sector that it is increasingly becoming easier to engage in hacking activities, due to the availability of easy-to-use and automated hacker tools.

### 3.5 IDENTIFYING HACKER MOTIVES, OBJECTIVES AND ETHICAL VIEWPOINTS

#### 3.5.1 Introduction

The discussion of the different hacker profiles set out in section 3.3 revealed that hacker activities are fuelled by a variety of motives or ethical viewpoints. These may range from anarchistic and violent behaviour to personal vendettas or simply the desire to become famous (Pipkin, 1997:4). The literature suggests that hackers might be bored and curious, seeking a challenge or taking revenge (Beaver, 2004:24) or they may simply be looking for community peer recognition (Arief & Besnard, 2003:12; Denning, 2006). They might try to sabotage their own hacker competitors, stealing identities or terrorising particular targets (Schell & Martin, 2004:2). More sinister objectives that they wish to pursue may include the need for financial gain. They are often very persistent or spend great amounts of time finding
a solution to breaking into a system (Young & Aitel, 2004:31). Greater complexity is only likely to increase their persistence. On the other hand, hackers may also break into a system for no particular reason. They might do it simply because they have the required skill (Beaver, 2004:25).

In an attempt to identify the motives and objectives of hackers, it is important to consider the criminal or personal nature of these motives and objectives. Highly motivated hackers, fuelled by some underlying personal motivation might be more dangerous. This is evident from the following two quotes:

Are hackers a threat? The degree of threat presented by any conduct, whether legal or illegal, depends on the actions and intent of the individual and the harm they cause (Kevin Mitnick as quoted in Basta & Halton, 2008:3).

They (hackers) flout the law by cracking into communication networks, copying and distributing copyrighted software and other intellectual works, caring nothing for the norms of common morality (Nissenbaum, 2004:198).

The underlying general psychology and motives of hackers will be discussed below, where after some of the specific objectives that hackers wish to achieve will be presented. This will assist with the identification of appropriate detective or preventative countermeasures.

3.5.2 General psychology and underlying motives of hackers

A hacker’s primary objective is to exploit a vulnerability or control weakness in a system or network, compromising one of the control objectives of information security (Graves, 2007:8) and so gaining access to a system. However, the underlying motives for doing so vary.

The literature suggests that there are a host of factors that may drive hackers: addiction to computers, curiosity for what may be possible, excitement, social status, peer recognition, power, and the betterment of society in the case of grey and white hat hackers (Tiller, 2005:35-36; Leeson, 2006:12; Steube, 2004:31, 34). The need to belong to a heterogeneous group of people with the same interest may be another important factor for hackers engaging in criminal activity (Krone, 2005a). The fundamental interest in technology poses an intellectual challenge for hackers. These factors are often shared by large social groups. Anonymity is often an important factor, since knowledge and experience are shared without personal knowledge of the originator (Arief & Besnard, 2003:11-12; Steube, 2004:31). Hacker activity is also conducted in secret, due to the illicit nature of the act.
Financial gain, sometimes leading to financial greed, is also a motivational factor (Bradbury, 2011:18).

It is important to consider that hacking is not only a purely technical activity. The literature shows that hacking is also about the imagination and the creative use of technology. Hackers find themselves in a virtual underground, interacting with individuals from different subcultures, and relying on their fellow hackers to complete complex hacks (Thomas, 2002:5-6; Holt, 2005:148). Research suggests that hackers often show an above-average intelligence (Stamatellos, 2007:17) that combines well with a creative instinct to find new ways of gaining access to systems. But in truth, most hackers are opportunistic in nature. They often make use of unsophisticated techniques to break into an organisation’s IT systems (Nagarajan, 2004). Hackers often boast skills which are non-existent. Nonetheless, they pose a real threat to organisations. Power and social status also lead hackers to wanting to prove themselves as being the best. This may include attacks against respected white hat hackers in the security community (McWilliams, 2002). This in turn could lead to feuds between white hat and black hat hackers. Hackers often enjoy the adrenaline rush of evading the authorities and receiving recognition from their peers (Tiller, 2005:34). They receive instant gratification when breaking into a challenging target (Beaver, 2004:24).

Research suggests that hacking is often regarded as a male-dominant activity, although research has shown that women also actively participate in hacker activity (Jordan & Taylor, 1998:767; Adam, 2003:3). There is a general tendency for young talented individuals to get involved in hacking. This could be a means of channelling their anger and frustration of their adolescent years into illegal activity. In some instances, this behaviour does stop and could even be used for legal purposes, such as in the case with white hat hackers (Schell & Martin, 2004:8-9).

Hackers often participate in the development of freeware tools used by the information security and hacker community. These projects give them a sense of enjoyment and fulfilment in contributing to the community (Lakhani & Wolf, 2005:4). Even though hackers get pure enjoyment from the intellectual challenge of breaking into a highly secured target (Krone, 2005a), they may also have technical motives behind their actions – for example, hiding their identities; obtaining administration rights on IRC chat lines; and stealing bandwidth and storing files without being charged for this service (Arief & Besnard, 2003:13).

From the information above, it is clear that the behaviour of hackers is complex. Hackers are sometimes seen as individuals with an addiction to computers, and lacking social skills to
interact with people of their own social stature. Some psychologists believe that hackers choose computers as a substitute for humans, in order to avoid the complexities of human relationships (Stamatellos, 2007:17).

Hackers’ own perceptions about their activities are perhaps best illustrated through the results of a survey conducted at the DefCon conference in Las Vegas in 2007 among self-proclaimed hackers, compared with results obtained from a control group at a university in the USA. For the purposes of that study, data was collected from attendees of the conference by means of a questionnaire. In total, 127 attendees completed the survey of whom 54 indicated that they were involved in illegal hacking activities, and the results from the questionnaire was immediately split between hackers and other attendees who completed the survey. For the control group, 136 undergraduate students at a US university completed the same questionnaire, with only one student indicating that he or she had ever conducted illegal hacking activity. The results obtained from the three groups (hackers, other conference attendees and students) were then categorised into “perception measures of interest”, which included the following five groups (Young, Zhang & Prybutok, 2007:282-286):

- **Moral disengagement**: This refers to the process of justifying illegal or unethical behaviour. If such behaviour is morally justified, the individual will start believing that his actions are ethical and socially acceptable. The survey results indicated that hackers have a significantly higher level of moral disengagement than the other survey participants. Hackers believe that hacking is acceptable as long as it does not cause any damage.

- **Informal sanction**: This refers to the reactions of other people impacted directly or indirectly by an individual’s unethical behaviour. Social pressure could be a deterrent to unethical behaviour. Survey results indicated that hackers do not fear being rejected as a result of the unethical behaviour. Instead, they expect praise or acceptance from their peers.

- **Punishment severity**: This relates to the impact on the individual when he or she is caught conducting his illegal activity. This includes both direct and indirect impact, e.g. prison time vs. inability to obtain employment. The survey indicated that hackers were well aware of the consequences of being caught for hacking.

- **Punishment certainty**: This is the likelihood of being caught. Individuals are more cautious when they know the likelihood of being caught is high. The survey results have shown that hackers have a high confidence level that they will not be caught. This explains why the consequences of hacking do not act as an effective deterrent.
•  **Utility value:** This is the gratification received from an illegal activity. The survey results indicated that hackers enjoy the fulfilment of hacking into a system. They may also seek monetary gratification, by selling the confidential information they have stolen.

The study concluded that various perceptions exist among hackers. The study highlighted that hackers believe hacking is acceptable and that their activity helps improve organisations’ system security. The study also found that hackers believe that, when caught conducting illegal hacking activity, their families would not negatively respond to this. Hackers tend to believe they will gain the respect of their peers. Another observation made by the study is that hackers perceive the consequences of being caught for illegal hacking activities as being very serious. Despite this, hackers believe that there is a low likelihood of being caught. Finally, the study highlighted the belief that hackers have more to gain from illegal hacking, as opposed to suffering losses due to illegal hacking (Young, *et al.* 2007:281, 284-286).

Importantly, organisations who seek to protect themselves against the threat of hacking must take note of the fact that many hackers believe that hacking into a system does not constitute a crime. In doing so hackers completely ignore the organisations’ policies and procedures. In fact, they show a complete “disregard or disdain” for the law (Cross, 2008:93). One of the reasons why hackers do not fear being caught is highlighted by Kshetri (Young, *et al.* 2007:286):

> Companies are often reluctant to report cybercrime either due to lack of confidence with law enforcement agencies or embarrassment for being the victims of cybercrimes.

Hackers see the creation of system accounts and gaining access to system passwords, when no physical damage was done, as a justifiable crime. As long as the files remain on the system and the system resources would have gone unused, they are of the opinion that no harm was done. Hackers often lack the maturity to see their actions in perspective. Hackers believe in the principles of free information for all and regard hacking as a process of gaining knowledge (Denning, 2006; Stamatellos, 2007:17).

### Thematological research questions

Based on the literature review above, the following thematological research questions can be defined:

**Hacker motives**

- The extent to which there is awareness in the banking sector that hackers may have different motives.
- The extent to which there is a realisation that hackers are highly motivated, which might make them even more determined to commit a crime in the banking sector.
Just as the underlying psychology and motives of hackers vary as they engage in these activities, so too do the specific objectives they wish to achieve.

### 3.5.3 Specific objectives of hackers

The literature suggests that there are a myriad of specific objectives that hackers wish to achieve. These objectives have a bearing on the lengths to which hackers will go, the amount of damage they may cause and even whether their actions will be identified by target organisations. Some of the common objectives that hackers seek to achieve are set out below.

#### 3.5.3.1 Hackers engaging in extortion or pursuing organised crime

One of the biggest driving forces for professional hackers is money (Leeson, 2006:21). Online organised crime is becoming a serious threat to society (Independent Online, 2006). As an indication of the organised nature of hacker activity, exploits and malware are being sold on the hacker underground. Malware can be defined as malicious software, such as viruses, worms, Trojan horses and malicious applets (Holt, 2005:2). At the lower end of the monetary scale, Trojan software, which is used to steal online account details, is being sold for anything between $1000 to $5000. Botnet software may be sold for between $5000 to $20000. The price range for exploits ranges from $4000 for a Windows Metafile exploit and goes up to $50 000 for a zero-day Windows Vista exploit. Other items on sale include credit card numbers with PINs, driver’s licences, birth certificates and social security cards (Naraine, 2006). Clearly it is a very lucrative business.

Due to the continued growth in Botnets, flaws in the inherent design of the Internet, and continued increase in software vulnerabilities, DoS attacks have become a threat for many organisations. Attackers could threaten an online business with a DoS attack, requesting payment from the victim. Companies are often willing to pay the extortionist, for fear of the possible reputational consequences (Gu & Liu, 2007:4, 9).

It is suggested that, similar to a “hired gun”, professional hackers (commonly black hat or über hackers) will sell their services to organised crime syndicates (Skoudis & Liston, 2006:8-9; Beaver, 2004:24; Krone, 2005a). One could find extortionists among hackers, who hold organisations at ransom to pay large sums of money for not divulging sensitive information about the organisation (Tiller, 2005:31). Hackers might also join forces with crime syndicates and may become actively involved in crime-related activities while covering
the tracks of the crime syndicate. These syndicates will look for sensitive data, launder money or conduct identity theft. They pursue any lucrative cybercrime activity (The Honeynet Project, 2004:510-511; Krone, 2005a). Crime syndicates are often very successful in their hacker activity and often operate in countries other than those that have any jurisdiction to legally prosecute the hacker. These countries might have a completely different set of laws (or lack thereof), with a lack of cross-national boundary co-operation or international laws facilitating extradition. This may lead to the prosecution of hackers being almost impossible (Bahadur, Chan & Weber, 2002:108).

3.5.3.2 Hackers engaging in hacktivism

The word “hacktivist” is derived from a combination of the two words, “hacking” and “activists”. It refers to hackers who feel it is their moral obligation to stop activities such as human exploitation, anti-religious activities or activities of a political nature (Wysocki, 2003:153; Osborne, 2006:277). For example, they may fight for animal rights or environmental issues (Young & Aitel, 2004:35; Skoudis & Liston, 2006:9). They may create a virtual “blockade” in cyberspace, blocking off supporters of a particular movement from gaining access to the target or supporters’ websites where relevant propaganda may be published, by means of DoS attacks, website defacements or malware distribution (discussed in section 3.9.6). This is referred to as a form of “electronic civil disobedience” (Zager, 2002; Taylor, 2005:634; Manion & Goodrum, 2007:61; Stamatellos, 2007:16).

Research has shown that hackers fuelled by these motives could also have more sinister intentions, for example engaging in anarchism or racism. They see the Internet as a place to promote their message and create public awareness (Wysocki, 2003:153; Beaver, 2004:23-24; Barber, 2001:16). They do not necessarily have the intention of breaking into a system.

Web-defacement is a popular technique used by hacktivists to convey a particular message (Pearce, 2002:14; Wysocki, 2003:155). In one example, on 13 September 1998, a hacktivist group defaced the New York Times home page in retaliation for a book authored by the New York Times reporter, John Markoff. In this book, Markoff describes the exploits and eventual arrest of Kevin Mitnick, who built up a reputation for his illegal hacking activities during the 1980s and early 1990s and who evaded the authorities for three years before being arrested in 1995 (Thomas, 2002:197-198).

Karatzogianni (2004:2, 3, 6, 15) argues that it is sometimes difficult to distinguish between cyberterrorism (discussed in section 3.5.3.5) and hacktivism. The political crisis in the Middle
East during 2002 led to defacement attacks on strategic Israeli websites. Physical conflict has been followed by virtual conflict on the Internet. Websites of Saudi Arabia, Egypt and Jordan have also been targeted during these attacks. The exact origin of these attacks is not known, although it is believed to be Egyptian (Leyden, 2002; Karatzogianni, 2004:11). Hacktivism is a growing threat, accompanied by even more sophisticated hacker attacks (McAfee Labs, 2010:6). Attacks of this nature slow down legitimate business and governmental Internet traffic.

### 3.5.3.3 Hackers engaging in vigilantism

Another motive driving the need to engage in hacking may be vigilantism. Vigilantism involves hackers who wage a war against what is called the “Internet’s lower life forms” (Shah, 2004:250; Tiller, 2005:30; Krone, 2005a), for example child pornographers or terrorist groups. Individuals who conduct vigilantism on the Web are also referred to as “cyber vigilantes”. Hackers engaging in vigilantism may launch an attack against the target offender. The attacks are mostly in the form of a DoS against the offender’s website (Schwartau, 1999).

Hackers with vigilante notions will go to extreme lengths to eradicate these crimes. Research suggests that both grey hat hackers (Pashel, 2006:198) and white hat hackers (Deisman, 2008:178; Everett, 2009:11) engage in vigilantism. A good example of a “virtual” vigilantism is taken from research conducted by Deisman (2008:178). A group called “Ethical Hackers against Paedophilia” claimed they worked alongside law enforcement to eradicate the distribution of child pornography. Their members had mentioned in interviews that they would at times hack into sites hosting child pornography, in order to delete the content (Deisman, 2008:178). According to Deisman (2008:179), since 2003 their activities went underground, for fear of retaliation by owners of these questionable websites.

### 3.5.3.4 Hackers engaging in industrial espionage

Industrial espionage is another specific objective for hackers. In particular, über hackers may be paid handsomely for stealing information about a competitor’s new product or service (Tiller, 2005:32). A hacker will plan this kind of attack with great caution, trying to create a regular entry point into the system for easy access over an extended period of time (Barber, 2001:16). These activities are all related to hacking as cybercrime (the latter is discussed in section 3.10).
3.5.3.5 Hackers engaging in terrorism

The threat of terrorism is a real concern in the 21st century. As the skills levels of the hackers of today increase, so too are their wrongdoings more carefully planned and often carried out with military precision (Pipkin, 1997:1). Whereas terrorists may use the Internet as a tool during their terrorist acts, cyberterrorism involves using the Internet and technology to attack critical infrastructure. Research suggests that due to the technical nature of these attacks, hackers are often role-players in such attacks (Matusitz, 2006:18, 19, 23; Veerasamy, 2010:3). Cyberterrorism is a growing threat that should be taken seriously by governments worldwide (Savino, 2006), as wars can also be fought on virtual battlefields. Cyberspace is regarded as the “fifth battlespace”, alongside land, see, air and space (Kingsley, 2011:20).

The literature suggests that terrorist groups may target critical infrastructure, for example the telecommunications infrastructure, financial systems, banks or governmental websites (Skoudis & Liston, 2006:8; Beaver, 2004:24; Veerasamy, 2010:4) with the intention of shutting them down or causing significant disruption on a global scale. Karatzogianni (2004:3) has labelled this kind of attack as “cyberconflict”, implying that a real-world attack could instigate “cyberwar” on the Internet among opposing parties. A hacker-led attack on power grid utilities could cause massive blackouts and possibly cripple an entire economy (Schell & Martin, 2004:23). Although there have been very few incidents of significant hacker terrorist attacks (Zager, 2002), they may play a bigger role in the future. The following are two examples of hacker terrorism attacks in the past decade:

- Hackers from China and Russia are believed to have gained access to US electrical grid systems during 2009. They could potentially launch an attack that could cripple critical US infrastructure (Gross, 2009). These attacks could spill over into South Africa, due to the strong economic relations with China. South Africa could be seen as a supporter of the Chinese government and its political beliefs (Jones, 2009).

- North Korean hackers are believed to be behind the attacks which slowed down several US and South Korean websites, such as Defence Ministry, National Intelligence Service and banking websites during 2009. Internet Service Providers (hereafter ISPs) hosting these websites had to take countermeasures to protect these and other business-related websites from cyber-attacks (Kim, 2009).

It is suggested that hacking is presently also used as a means of financing terrorism, by means of, for example, stealing credit card numbers and using the credit card numbers to secure funding (Lormel, 2007:3, 15). As a countermeasure, military and secret services are employing hackers to help secure countries against hacker attacks. Hackers may not only...
defend “mission-critical systems”, but may also launch attacks against the offence (McMichael, 2008). President Obama has approved an executive order that allows the US Military to counter hacking techniques and cyber-attacks, as an official military attack mechanism. The attack techniques could range from blocking cyber-attacks from other countries, to attacking opposing countries’ defence networks (Seidl, 2011).

3.5.3.6 The objectives of hackers who find themselves inside organisations

Hackers often launch their attacks from outside organisations, but the literature suggests that attacks from inside organisations are also prevalent and could be equally disruptive as those initiated from outside (Skoudis & Liston, 2006:9; Young & Aitel, 2004:50-51). These include attacks from insiders who are often disgruntled employees and who carry a wealth of information regarding the internal network and application environment (Pipkin, 1997:4; Arief & Besnard, 2003:2; McCumber, 2005:60). In fact, insiders may perform these attacks for various reasons (Aeran, 2006:15-20):

- Financial gain (e.g. manipulating personal records).
- Revenge (due to negative feelings towards the organisation).
- Espionage.
- Emotional distress (e.g. due to personal circumstances).
- Desire for respect.
- Recurring decision failure (e.g. constant disapproval by the manager).
- Mental disorders.
- The challenge itself or pure curiosity.

Insiders may also on occasion collude with other criminals, such as syndicate members. One of the biggest insider cybercrimes took place at Vodacom, a South African cellular service provider during 2009, where an employee assisted two Nigerian syndicate members to divert Internet banking SMSs to the syndicate members to ensure that online banking transactions could be completed illegally. Syndicate members made use of phishing to obtain online banking accounts credentials, such as account numbers and passwords, before commencing with the online banking transactions. The total losses affected clients suffered for this crime were estimated in excess of R7 million (Lieberum, 2009; Nkosi, 2009).

One of the primary reasons why insider attacks are so successful when compared to external attacks is their ability to bypass physical and technical security controls without much effort. Firewalls, Intrusion Detection Systems (hereafter IDS) and physical security
measures are installed to protect the organisation from outside attackers, but not from hackers within (McCumber, 2005:60). This lack of focusing on security on the internal network is one of the major reasons behind internal attacks still being very successful today (Delahunty, 2011). Brancik (2005:28) points out that the characteristics of insider attacks vary greatly and it may therefore be problematic to define a rule-base for an internal-facing IDS. Insiders will be familiar with internal policies and procedures, and will also be familiar with vulnerabilities and flaws in the IT systems (Cappelli, Moore, Shimeall & Trzeciak, 2006:4; Darragh, 2009:14) and they might ignore or circumvent the internal policies and procedures to their advantage (Brancik, 2005:24, 256). Insiders often have full access to the network and other sensitive systems (McCumber, 2005:60; Jones, 2008:220; Richards, 2009:45). This could lead to unauthorised changes to production software.

The effect of the insider threat is further demonstrated by the third research study conducted by the Computer Emergency Response Team (hereafter CERT) and the US Secret Service (hereafter USSS), at Carnegie Mellon University into the prevention and detection of insider threats. The first study defined twelve practices to be followed by organisations in preventing or detecting insider threats. The second study added a focus on malicious insider activity. This study is a continuation of the previous two studies, providing new insight on the same topic. Insiders are a particular threat that is taken very seriously by the US DoD and USSS, and the significance of the threat can be understood when a country’s primary defence is threatened. Information on a total of 250 actual insider threat cases was collected. A hundred and fifty of these cases were provided by the USSS for the second research study. An additional 100 cases were added by Rosenthal from the Software Engineering Institute’s Library Services for the latest study (Cappelli, Moore, Trzeciak & Shimeall, 2009:10). Since a number of the cases did not have enough detail or were still pending legal proceedings, a total of 190 were selected for the study (Cappelli, et al. 2009:4, 11). The results of the study, also depicted in Figure 3.2, are categorised and discussed by class of malicious insider activity:

- **Theft or modification for financial gain:** This class includes current and former employees, contractors and other business associates who misused or compromised levels of network access to steal or modify organisational information for financial gain. A total of 77 out of a 190 (41%) cases fell into this category. Of the 77 cases, 72 were found to be current employees at the time of the criminal activity. The criminal offences were mostly committed by junior staff members. The root cause of this activity is financial gain. As with the Vodacom incident presented earlier, two-thirds of the cases involved collusion between insiders and outsiders. The impact of the cases investigated ranged from negative publicity to losses of up to $20 million (Cappelli, et
Theft or modification for business advantage: This class includes current and former employees, contractors and other business associates who misused or compromised levels of network access to steal confidential or proprietary information to gain a “business advantage”, such as starting a new business. A total of 24 cases out of 190 cases (13%) fell into this category. Of the 24 cases analysed, 71% of perpetrators were employed in technical positions. A total of 75% were current employees. In most cases (88%), the employees already had access to the information before perpetrating the theft (Cappelli, et al. 2009:21-22).

The report highlights the likelihood of the insider threat, in particular where reliance is placed on IT infrastructure. The report goes on to provide best practice advice for the prevention and detection of insider threats (Cappelli, et al. 2009:24, 27-31). Some of the crimes listed above relate to cybercrime, which will be discussed in section 3.10, where the close relationship between hackers and cybercrime in general will be presented.

Importantly, it must also be borne in mind that the risk of uneducated employees who disable local security on their PCs, download viruses from the Internet and run hacker tools without authorisation is as high as that presented by educated insider hackers.

Similar to the research conducted by Cappelli, et al., research conducted by Zager and Brancik also indicated that insiders who present a risk include vendors, contractors, consultants and temporary staff who do not have any particular loyalty to the organisation and yet have a great deal of access to systems and data (Zager, 2002; Brancik, 2005:25). Vendors often install backdoors or even security flaws in their software, which allow them access back into the system at a later time.
Thematological research questions

Based on the literature review above, the following thematological research questions can be defined:

**Hacker threat**
- The extent to which there is recognition, specifically in the banking sector, that the threat posed by hackers inside a bank is high.
- The realisation that hacktivists could cause damage to the reputation of the banking sector.
- The extent to which the banking sector could protect itself against industrial espionage.

**Hacker profiles**
- The extent to which a banking employee in a highly technical position may start showing an awareness of the characteristics and activities associated with hackers.

**Hacker motives**
- The extent to which there is an understanding in the banking sector that hackers may have a range of specific objectives that they may wish to pursue.
- The extent to which there is an understanding in the banking sector that hacktivists’ ethics and skills levels may vary.

**Hacking response**
- The extent to which the banking sector believes that a range of safeguards is needed to protect them against hacker attacks given the range of objectives and motives pursued by hackers.

3.5.4 Conclusion

There is no single motive behind hacker attacks. Motives vary from social recognition and status to criminal intent and financial gain. Similarly, as regards the specific objectives that hackers hope to achieve, there is again an array of options underlying the actions of hackers, from terrorism to the need for espionage. The wide scope of motives and objectives that hackers have makes it more difficult for those who want to protect themselves against the threat of hacking to put adequate countermeasures in place. This situation is further exacerbated by the numerous weaknesses that facilitate hacker attempts, as well as the range of hacker techniques available.

On the more positive side, at least there is a common hacker methodology and basic tools and technologies required in the process that provides some common clues as to how organisations can protect themselves against the threat of hacking. A common hacker methodology will be discussed in section 3.6, and the basic tools and technologies used to perform hacker attacks will be presented in section 3.7. Thereafter, the weaknesses that facilitate successful hacking attempts will be discussed in section 3.8, while a range of hacker techniques will be dealt with in section 3.9.
3.6 A COMMON HACKER METHODOLOGY

Hackers do not necessarily follow a structured methodology when planning an attack. Nonetheless, an experienced hacker will engage in some form of preparation for an attack, as opposed to script kiddies who might launch an attack without any preparation (Skoudis & Liston, 2006:183). Most hackers would at least engage in some of the following steps or phases, which follow in a logical sequence (Skoudis & Liston, 2006:183, 239, 339, 547, 627):

- Reconnaissance.
- Scanning.
- Gaining access by launching an attack.
- Maintaining access.
- Covering tracks.

The first phase, reconnaissance, involves the gathering of publicly available information, which will help the hacker plan the attack. The information collected could include a profile of the organisation, who the administrators are, details about internal processes such as the helpdesk function and details about the network and systems used in the organisation (Young & Aitel, 2004:58). This information can be obtained via social engineering techniques, such as calling random employees in the organisation and soliciting information that may be used to further advance the attack against the organisation, often focusing on non-technical means of bypassing security measures. Another technique is dumpster diving, which involves looking for confidential details thrown away in the organisation's dustbins, or searching for relevant information on the Internet (Thornburgh, 2004:133; Skoudis & Liston, 2006:184, 193, 195; Frangopoulos, 2007:65). The implication of all these steps is that hackers will not limit their activities to virtual or logical information for access, but could also attempt to gain unauthorised physical access by means of a stolen access card to an organisation's premises to obtain information that they require (Frangopoulos, 2007:68).

The second phase, scanning, involves mapping out the target and finding potential vulnerabilities. Scanning can include wardriving, to identify unsecured wireless networks accessible from outside an organisation's premises, wardialling, to find open modems connected to the network, and "network mapping", to discover accessible routers and servers (Skoudis & Liston, 2006:239, 240, 254, 261). Once a number of target systems have been identified, port scanners will be used to detect open ports and services on the target server or router. Vulnerability scanners will be used to identify software or service
vulnerabilities (Young & Aitel, 2004:79). Since some scanning tools test for default passwords, scanners may disrupt or damage IT applications and it may be possible for hackers to obtain unauthorised logical access to a target's system during this phase.

During the third phase, the actual attack will be launched. The primary objective is to gain access to the system or network. A hacker would patiently launch his selected attack, with the hope that it will be successful (Skoudis & Liston, 2006:339). Should the first attempt fail, the hacker might postpone the attack until later to avoid detection. Either the same attack or a different attack can be used, but unauthorised logical access would remain the primary objective. The attack may also result in IT disruption, theft and damage to software and data. The attack could also lead to web defacements for peer recognition (Woo, Kim & Dominic, 2004:64), or a misuse of business applications or fraud. This may be accomplished by escalating their system privileges (circumventing segregation of duties in the process) or obtaining full administrator access to an operating system (Harris, et al. 2005:83).

The fourth phase involves maintaining access by installing Trojans, backdoors or rootkits, the last being a collection of software that can be used by the hacker to, for example, crack the administrator password and clean log files (Skoudis & Liston, 2006:547, 548: EC-Council, 2008b:935). Clearly, in this phase the hackers will misuse the target's systems, possibly planning for further attacks. During this process, data and software may be altered and even destroyed. Theft of commercially valued data could also be a primary objective once access has been obtained. The hacker might return again, to access a business application for criminal purposes (Protalinski, 2008) or to achieve other cybercrime objectives, such as storing inappropriate material.

The last phase involves cleaning up any evidence that access has been gained into the target's system to allow the hacker to remain undiscovered and use the system for as long as possible. In this phase, the hacker could alter application and operating system log files to delete any signs of his activity (Skoudis & Liston, 2006:627-628).

As each of the phases in the hacker methodology is so distinct, countermeasures for each phase should be considered as part of an overall hacker threat strategy.
Thematological research questions

Based on the literature review above, the following thematological research questions can be defined:

Hacker threat
- The extent to which there is an understanding in the banking sector that a common hacker methodology exists.
- The extent to which there is an understanding that each phase of the methodology holds a different threat, which may disrupt a bank.
- The extent to which the banking sector realises that a hacker may covertly access the bank’s systems and remain hidden indefinitely.

Hacking response
- The extent to which there is agreement that specific countermeasures should be put in place to protect the banking sector against each of the steps in the hacking process.

3.7 BASIC HACKING TOOLS AND TECHNOLOGIES USED BY HACKERS

Hackers are highly proficient in the use of technology, and ironically the most inexpensive equipment and tools could be used in a hacker attack, even while organisations invest a substantial amount of money to protect them from the threat of hacking. At a minimum, hackers need access to PCs, the Internet, possibly network equipment, various software packages and operating systems in order to carry out hacking activities. PCs are generally inexpensive nowadays, while access to the Internet might be the most expensive component.

A particular operating system that is favoured by the hacker community is Unix (Pipkin, 1997:6). Unix is in widespread use in universities and research laboratories. Consequently, information about Unix is easily obtainable and well documented. Unix is predominately used in a client/server environment. However, generally this type of software requires expensive equipment, placing it out of reach of most hackers. Its “desktop” counter, Linux, has therefore become a very popular alternative in the hacker community (Tiller, 2005:16, 166). Linux is free, easily obtainable and very powerful. Many of the freely available hacking tools are written for the Linux operating system environment. Red Hat Linux (the name of one of the various Linux operating systems available) is a popular Linux open source operating system (Beaver, 2004:194). Perhaps less user friendly compared to an operating system such as Windows XP, it offers more functionality, which a hacker might find useful.

Hackers study the source code of operating systems and have in-depth knowledge of network protocols. Unix, Linux and many of the security/hacking freeware tools are written in...
the programming language C or C++. Not surprisingly, these languages are very popular in
the hacker community (Young & Aitel, 2004:191; Schell & Martin, 2004:53). Other
programming languages frequently used by hackers are C#, Java, Perl, Python and Visual
Basic (Young & Aitel, 2004:190-192).

According to Pipkin (1997:6), hackers do in-depth research to understand the risks and
vulnerabilities associated with a particular operating system or security tools used to protect
the system. This process also includes the reading of security bulletin boards from
professional organisations, for example CERT. Hackers also make extensive use of open
source hacking tools. Open source software is software whose source code is open and free
for use and modification by the general public, without restriction. The software is distributed
under licences which specify copyright rules, to ensure for example that the code remains
open source, even when incorporated in commercial products. One example of such a
licence is the general public licence (hereafter GPL) (Behlendorf, 1999; Mudeliar, 2008:18).

Hacking tools refer to software that supports one or more of the phases discussed in section
3.6, such as Nmap, a port scanning and network discovery tool (Han, 2003:12). Hacking
tools automate some of the tasks carried out by the hacker against the target system, during
his attack. Thousands of open source hacking tools are freely available and widely
distributed on the Internet (Fried, 2006:411). Hackers search for existing hacking tools that
will perform the intended function they wish to carry out, before attempting to develop the
tools themselves (Lyon, 2011). Often, the required tool will be available for download and
hackers could start using it immediately.

Hackers also make extensive use of hardware devices such as modems, wireless network
cards, antennas, routers and key loggers during their attacks. It is possible to buy these and
other technical devices, including comprehensive how-to guides and CDs with collections of
Particularly in the USA, Internet access has become very affordable. Some ISPs even offer
free Internet access, although the reliability of these services might be questionable. This
does however create a basic launch pad for aspirant hackers.

Linking the common hacker methodology with the basic tools and technologies that are
freely available to hackers, their attempts are further assisted by a range of weaknesses that
facilitate successful hacking attempts.
Thematological research questions

Based on the literature review above, the following thematological research questions can be defined:

**Hacker threat**
- Whether there is an understanding in the banking sector that hackers may be able to apply their trade by using easily accessible and affordable equipment.
- Whether there is an understanding in the banking sector that hacking tools are freely available, easily accessible and developed for a particular hacker task.
- Whether there is an understanding in the banking sector that hackers can gain knowledge of source codes and programming languages, as they are easily accessible.

### 3.8 WEAKNESSES THAT FACILITATE SUCCESSFUL HACKING ATTEMPTS

#### 3.8.1 Introduction

It is suggested in the literature that several factors contribute to successful hacking attempts. Hardware and software have become more accessible to the general computing community, as opposed to being confined to large corporations or research institutions. More individuals are exposed to computers from an early age, and computer systems are increasingly easier to use (Kovacich, 1998:132-133). The availability of information to the public has also led to an increasing awareness of known vulnerabilities, as pointed out by Harding (2002):

> Most hacks involve well-publicised vulnerabilities applied indiscriminately across many machines. Hackers are opportunistic, and machines are generally targeted for their connectivity rather than any information that may reside on that machine or any attached network.

Script kiddies may use well-known exploits and scan thousands of machines connected to the Internet, until one vulnerable machine is found. Alternatively, an attack might be more targeted at a specific host, where the hacker might use a variety of exploits and techniques to break into the target (Harding, 2002). Weaknesses that could be exploited include poorly configured Web servers, old or un-patched software, disabled security controls, and weak or default passwords (Palmer, 2001b). Rather than identifying an exhaustive list of weaknesses, which may facilitate successful hacking attempts, a possible approach is to identify broad categories of weaknesses, which will be used to facilitate the discussion. To begin with, the broad categories are identified on the basis of a review of a number of literature sources.
3.8.2 Identifying broad categories of weaknesses that facilitates hacker attacks

Authors have different opinions as to the various categories of weaknesses that may lead to successful hacking attempts. Lam, LeBlanc and Smith (2004:6) list the following reasons for network security failure: human and policy factors, misconfiguration, poor assumptions, ignorance and failure to stay up to date. Several of these relate to human fallibility. In their model for threat classification, Farahmand, Navathe, Sharp and Enslow (2005:203-225) classify hacker techniques into physical, personnel-related, hardware, software and procedural categories.

Then again, others suggest that weaknesses are not always technical in nature. Authors such as James (2006:420), Long (2007:239) and Harris (2005:362) highlight the physical access weaknesses that may lead to successful hacker attacks. Harris (2005:362) argues that physical security weaknesses could lead to theft, interruptions of operations, damage to equipment, compromising system security and unauthorised access.

Another commonly exploited weakness is logical access controls, typically in the form of a username and password combination. Other authors, such as Thorsheim (2006:1050) and Harris (2005:214-216), also highlighted this area of weakness. Vulnerabilities associated with both software and hardware are another common weakness exploited by hackers. Siegel, Sagalow and Serritella (2006:1750) point out that operating systems, networks and applications could all have vulnerabilities. Similar views are shared by Harris (2005:318).

Research conducted by Thorsheim (2006:1049) and Siegel, et al. (2006:1750) highlights that weaknesses associated with networks may lead to successful hacker attacks. Thorsheim (2006:1049) points out that hackers could get access to internal networks via unprotected remote access servers (hereafter RAS) or due to a lack of network controls. Harris (2005:50) furthermore suggests that the Internet, extranets and intranets of organisations increase the complexity of their IT environments and the business processes they support. The Internet “opens the floodgates” to many potential risks. Kuegah (2006:19) agrees that the complexity associated with networks increases the likelihood of successful attacks. Fried (2006:411-412) highlights that many companies’ employees may not fully comply with the organisation’s defined policies and procedures. This speaks to human fallibility. Fried (2006:412) goes on to highlight the fact that many system administrators do not keep their systems up to date with the latest software patches. The resulting software vulnerabilities lead to successful hacker attacks. Like Fried, Wiles (2007:44) highlights the likelihood of social engineering being successful, due to human nature and management not assessing.
the likelihood of social engineering attacks succeeding. Kleen (2001:1.5) highlights software application weaknesses that may be exploited by hackers.

Based on the views presented above, the broad categories of weaknesses applied in this thesis are: physical access; logical access; software and hardware vulnerabilities; network connections and the human factor. Each of these will be discussed in turn.

3.8.3 Weaknesses associated with physical access

From the definitions of hackers and hacking presented in section 3.2.4, it can be inferred that the goal of a hacker is to break into a system. Even though hacking is typically associated with breaking into systems via electronic means, more direct approaches such as gaining physical access to IT equipment (The Honeynet Project, 2004:566) to break into systems are often very successful and the absence of, or weaknesses in, physical access controls could contribute significantly towards a hacker’s success. In this regard there are three areas of weaknesses which feature most prominently in the literature: weaknesses associated with physical access itself, the mobility of computing, and wireless networks; each of which will be discussed in turn.

3.8.3.1 Hackers obtaining physical access to a premises

As regards physical access, hackers could use innovative ideas to enter physical premises by, for example, attempting to gain entry to the premises via a side door or loading dock, as opposed to through a front entrance that might be well secured (Kevin, David & Ben, 2004:256). Hackers may also make use of the social engineering technique “tailgating”, to gain physical access to the premises, when more than one person enters a room at the same time. Even when more sophisticated physical access control mechanisms are being used, for example biometric devices, another person might enter the room together with the authenticated individual by using tailgating (McLean, 2003:71; Kevin, et al. 2004:256; Frangopoulos, 2007:68). In fact, Stamm argues that the mere existence of a database that contains biometric data would attract hackers, since the process involved in obtaining the biometric data and ensuring authenticity is more complex, allowing the hacker a longer time to use the compromised credentials. On the other hand, a password when compromised can be easily changed (Stamm, 2007:348). Sophisticated physical access authentication mechanisms are therefore not foolproof. Once inside the target organisation, hackers can put key loggers (a device connected to the keyboard port on the back of a PC, used to capture keystrokes as they are typed) and sniffers in place on unattended PCs to obtain user
credentials. They may also steal any type of removable media which may contain sensitive data or IT-related information, such as network diagrams or system details (Graves, 2007:170-171; EC-Council, 2008b:1339). None of these actions requires any technical skills.

Breaching the physical access controls might inevitably lead to theft of computer equipment. The information stored on computer equipment is usually of significantly higher value to the business than the cost of the equipment itself. For example, confidential data or commercial software code with considerable business value may be stored on the computer devices. Equipment might also be tampered with, leading to processing errors or unavailability of systems, consequently disrupting business operations (Graves, 2007:170-172). Theft of backup media could lead to an inability to recover from a potential disaster, affecting the ability to restore the operations of the organisation (Craig, 2001:153).

3.8.3.2 Hackers circumventing physical access by accessing mobile computing devices

The second area of physical access weaknesses relates to mobile computing. The bewildering pace of technological advancement has introduced several new IT devices, which make life both simpler, while at the same time introducing unique new risks. Universal serial bus (hereafter USB) storage devices have emerged in the last decade, replacing old legacy storage media, such as floppy and stiffy drives. These devices are commercially available in various storage sizes, ranging from one gigabyte to external hard drives with a capacity of two terabytes (or more). The inherent weakness of this technology is that it has not been designed with security in mind. USB storage devices have three primary risks associated with them. The first risk is associated with the propagation of malware. Many worms and viruses are programmed to copy themselves onto a USB memory stick, and to spread once the USB is connected to another PC (Lumension, 2009:3). The second risk is linked to the nature of the data stored on USB storage devices and the mobility of the devices. Confidential corporate data can be stored on these devices and an employee might carry it with him in public places such as shopping malls, airports and hotels, where it may be lost or stolen. An employee can also use a USB storage device to move files between a work PC and home PC. This data is susceptible to theft by both hackers and other criminals alike. A USB storage device could also lead to identity theft, when employees leave their own personal details on the device (Olatilu, 2006:27-28; Friedman & Hoffman, 2008:167; Lumension, 2009:3). Thirdly, hackers can install a fully functional operating system and hacking tools on a USB storage device and would be able to launch an attack from any PC, leaving no trace behind of their attack, as the operating system and software is not on the
PC itself (Kevin, et al. 2004:256; Lumension, 2009:4). Of particular concern here is the size of the data that can be stored on USB storage devices. It is possible to copy an entire customer database to such a device. In the past, this kind of data would have exclusively resided on a server’s hard drive or back-up tapes, which were handled securely within the secure confines of an organisation’s physical premises. USB storage devices take these huge volumes of data outside of the physical security controls of an organisation.

USB storage devices are not the only portable devices that pose a risk. Mobile devices such as cellular telephones, smart phones, PDAs and Blackberry devices could contain sensitive corporate information, such as employee contact details, corporate e-mails and also confidential data and files. These devices are not always enabled with logical access security and contain access pathways, such as 3G and WiFi, which could allow a hacker to access them remotely. Obviously the physical theft of these devices is also a major concern (Boni, 2008:5-6).

### 3.8.3.3 Hackers circumventing physical access via wireless networks

The third area of physical access weakness is related to wireless networks that extend an organisation’s network perimeter beyond the physical building. Whereas a physical network will be protected inside the walls of an organisation, a wireless network has no physical protection. This lack of physical security can allow hackers to identify available wireless networks through attacks such as wardriving, which is a technique that allows a hacker to drive around while attempting to connect to available wireless networks in the vicinity (Ashley, 2004:43-44). Randomly placed or poorly configured wireless access points could also lead to unauthorised access (Decloedt & Van Heerden, 2010:7). In 2005 Abdullah conducted a study into the intrusion security risk associated with wireless networks and the mitigating response, using NetStumbler (a hacker tool used to detect wireless networks). The location was the V&A Waterfront, a large retail centre in Cape Town, South Africa, where he identified 124 wireless networks, 30 of which did not have security encryption (such as Wired Equivalent Privacy, hereafter WEP) enabled. In general, he concluded that the security of wireless networks is a critical problem (Abdullah, 2006:149-150, 152, 153).

More and more organisations also allow their employees to work from home. In order to do that, typically, these employees’ PCs would be equipped with wireless network cards or 3G, which will allow them to connect to the nearest wireless network service provider. Wireless network cards further exacerbate the risks associated with the mobility of computing, in that the employee operates outside of the physical security controls of his organisation.
Therefore, as the traditional boundaries of organisations expand beyond their physical walls, the resulting potential weaknesses in physical access controls increase the likelihood of successful hacker attacks, whether by insecurely configured wireless networks or mobile computing devices and storage media.

### Thematological research questions

Based on the literature review above, the following thematological research questions can be defined:

**Business risk**
- The extent to which there is a clear understanding in the banking sector that the risks associated with physical access will increase the risk of hacking.
- The extent to which there is a clear understanding that organisational data is frequently situated outside of the physical walls of banks and that it could increase the likelihood of hacking.

**IT risk**
- The extent to which there is a clear understanding that wireless networks extend the perimeter of banks that must be controlled outside of their physical buildings.
- The extent to which there is a clear understanding that mobile computing devices can increase the likelihood of hacking in the banking sector.
- The extent to which the banking sector prohibits or controls the use of USB storage devices, for fear of loss of confidential data.

### 3.8.4 Weaknesses associated with logical access controls

One of the most fundamental controls implemented by an organisation to ensure system security is logical access controls (Lessing, 2006:114). Logical access controls ensure that only authorised users are granted access to systems and data (Van Niekerk, 2005:229). Logical access controls consist of components to ensure identification, authentication and authorisation. This is typically accomplished by making use of a username (identification) and password (authentication) combination (Harris, 2005:127-128). However, various other technologies can also be used to implement logical access, such as biometric devices, tokens and smart cards (Diakite, 2008:49). Biometric devices have not been widely implemented, due to the cost associated with the devices. Therefore, traditional usernames and passwords are still widely used (Farmer, 2006:46).

Hackers specialise in exploiting the weaknesses associated with password controls (James, 2006:419). When weaknesses in password management policies persist, this leaves an organisation vulnerable to an attack (McKay, 2006). Examples of password mismanagement include the use of default passwords, such as vendor-defined passwords for software. Making use of a password-naming scheme that is generally known might also lead to the
discovery of passwords (Heikkila, 2009:46). Although it is commonly known that basic password controls would not be enough to protect sensitive data, this might be the only or last defence against an encroaching hacker, in particular where the hacker has managed to circumvent for example the physical access controls (James, 2006:419).

The most common weakness associated with passwords is the lack of appropriate password strength. A password should be easy to remember, which may lead to the selection of easy-to-guess passwords (EC-Council, 2008b:792). Consequently, there is a trade-off between the associated risk and the strength of the controls: the greater the risk, the stronger the control should be, equally so for password controls. The username and password combination should also grant a user access to a particular system or particular level of access or system privileges. The weaknesses associated with an administrator password would relate to granting the user full unrestricted access to the system (Singleton, 2008:11-12). Hackers consequently target administrator accounts, since they provide the highest level of access to a particular system.

Some of the common design flaws associated with password complexity are, for example (ArticSoft Technologies Ltd. 2008):

- Commonly used or dictionary words.
- Repeating letters or numbers, such as 99999.
- Allowing short passwords (six characters or fewer).
- Failure to change the password at regular intervals.
- Storing passwords in clear text.
- The lack of lock-out functionality after several (usually three) unsuccessful attempts.

From the literature above, it is clear that password weaknesses are an essential contributor to weak logical access controls and need to be considered as such from a hacking risk perspective.

<table>
<thead>
<tr>
<th>Thematological research questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Based on the literature review above, the following thematological research questions can be defined:</td>
</tr>
</tbody>
</table>

**Hacker threat**
- The extent to which there is an understanding in the banking sector that hackers successfully exploit password control weaknesses.

**Hacking response**
- The extent to which there is an understanding in the banking sector that the risk associated with a
3.8.5 Software and hardware vulnerabilities

Up to this point, physical access weaknesses and weaknesses associated with logical access controls have been covered. A third area of weakness that facilitates successful hacking attempts is software and hardware vulnerabilities. In particular, software vulnerabilities found in operating systems and other software packages are attractive targets for hackers (Holt, 2005:98). They significantly increase the likelihood of organisations being susceptible to hacker attacks. Vulnerabilities can be defined as follows (Landoll, 2006:34):

… a flaw or oversight in an existing control that may possibly allow a threat agent to exploit it to gain unauthorised access to organizational assets.

A vulnerability therefore leads to the exposure of an organisation's assets, which could include IT systems and data. The National Institute of Standards and Technology (hereafter NIST) defines a vulnerability as a flaw or misconfiguration of a system that may lead to the eventual exploitation of the weakness (Wack, Tracy & Souppaya, 2003:13). Harris (2005:969) defines it as the lack of a safety measure which can be exploited. A broader definition of the possible scope of vulnerabilities is provided by Herrmann, who focuses on where vulnerabilities could reside, such as in system's hardware, software, communications equipment, operational procedures, and operational environment. Herrmann also indicates that vulnerabilities can result from either accidental or malicious intent (Herrmann, 2002:100-101).

Software vulnerabilities are seen as a main contributing factor to successful hacking attempts (Beaver, 2004:10). Designing software is not an easy task. In fact, there is no "silver bullet" to software engineering (Brooks, 1987:10). The complexity of programming and the various ways of representing the same principle in a programming language will eventually lead to errors. Both application software and operating systems could contain software flaws (Day, 2003:134). Security features and controls are often included as an afterthought, rather than including them in the development phase of software (Anderson, 2001:504). Software is developed by fallible humans, who often introduce errors (Macdonald, 2002:110). Wespi also shares similar concerns, by highlighting that software developers continue to develop vulnerable software. He also emphasises that due to the ease of automated attack tools, system administrators need to be more diligent in mitigating software vulnerabilities (Wespi, 2005:118). The testing phase of a software development
project should focus on security testing to ensure there are no common software vulnerabilities, such as overflow or injection flaws and poor input validation, which may be exploited by hackers (Paul, 2009:5).

It is also suggested that hackers are constantly on the lookout for press releases and public announcements of the latest software vulnerabilities and use the information to write new hacker tools or exploits. From this perspective, software vulnerabilities are a major concern within the information security industry (Brandt, 2003). These software vulnerabilities are subsequently exploited by hackers, allowing them to gain access or manipulate data on organisations' systems (Day, 2003:132; Krone, 2005b; Zhao, 2007:62). Increasingly, hackers are targeting vulnerabilities in applications, rather than vulnerabilities in operating systems and networks, since applications can provide easier access to financial reward (Kayle, 2010; Leech, 2010:8, 14). Le Grand and Sarel argue that software vulnerabilities can be found in web pages, e-mail applications, file transfer utilities, operating systems and database management systems. Although software vendors often provide patches to update their vulnerable software applications, organisations are not always effective in applying those (Le Grand & Sarel, 2008:27). This allows hackers to exploit software vulnerabilities, even long after the vulnerability has been publicised. Poor change control procedures could increase the likelihood of hacker attacks. IT administrators should patch their systems, to ensure all system vulnerabilities are closed. At times, it is not practical to keep up to date with the latest patch, since business applications might become unstable due to changes in the operating system. IT administrators might also be too busy to update their systems. Nonetheless, an unpatched system is vulnerable to hacker attacks (Harris, et al. 2005:64). Inevitably, it is also possible that outdated software and hardware remain in use, with neither of them being updated with the latest patches or software updates. Vendors might stop supporting a particular piece of technology because they have known or unknown vulnerabilities, which are easily exploitable by hackers (Singel, 2008; Dynamic Solutions Group, Inc. 2009). Organisations can of course protect themselves by implementing a rigorous patch management programme and subscribing to vendor update services, to ensure they address critical software vulnerabilities.

In-house-developed software solutions may also contain software vulnerabilities; however, they may not be publicly known. It is important to note that, increasingly, organisations are using web-applications and technologies as platforms for in-house-developed software (Van Woudenberg & Van Niekerk, 2010:3). This despite the fact that the World Wide Web and the technologies that support it were not originally designed with security in mind (Stamm, 2009:3). Hacker attacks might start off by focusing on network infrastructure and commercial
applications, but could also use certain attack techniques, such as buffer overflow attacks and race conditions (discussed in section 3.9.1.1) against custom or in-house-developed applications. Web-based applications also often include coding and scripting errors, which are exploitable by hackers (Ollmann, 2007). Hackers might have to spend more time and effort, finding vulnerabilities in in-house-developed software; however, the likelihood of hacker attacks remains high and organisations should thoroughly test their software solutions (De Villiers, 2010:25; Van Woudenberg & Van Niekerk, 2010:3, 6, 13, 45).

The latest software vulnerabilities and possibly exploit codes may also be for sale in the market to the highest bidder. A former controversial website, named www.wabisabilabi.com, started a marketplace for zero-day exploits and software vulnerabilities during 2007 and 2008. What was unique about this particular website was that it was not a covert underground website. It was instead a commercial website for both hackers and security specialists alike. It was alleged that it had been created with the intention of rewarding the work of white hat hackers, who might avoid selling their exploits to criminals (Naraine, 2007). The downside of such a website is that it significantly increases the probability of black hat hackers finding an exploit which will ensure a successful attack. The origin of these software vulnerabilities is also most likely the hacker community, discovered during actual hacking activity (Andreatta, 2007). It is therefore questionable whether knowledge about the software vulnerabilities was obtained using legal means. Although organisations could purchase the software vulnerabilities to protect themselves from hacker attacks, hackers could also buy it to launch a successful attack against an organisation. In particular, cybercrime syndicates will not mind paying significant amounts for zero-day exploits. Regardless of all the controversy associated with this website, there was only limited interest in purchasing exploits from this website. Consequently, the website was closed down (Lemon, 2008).

There has also been an increased interest in the concept “cloud computing”. Although arguably a cloud-computing environment would be highly secure, software or hardware vulnerabilities may exist in this environment, which in turn may be exploited by hackers (Gadia, 2009:24, 27; Grobauer, Walloschek & Stöcker, 2011). It is possible that in the future, cloud computing centres will host hundreds or even thousands of potential clients, due to ease of scalability of this kind of infrastructure (Cagle, 2008; Holownych, 2011), significantly increasing the potential exposure as a result of hacker breaches.
Thematological research questions

Based on the literature review above, the following thematological research questions can be defined:

**Hacker threat**
- The extent to which there is an understanding in the banking sector that hardware and software solutions used by the banking sector may contain software vulnerabilities, which are exploitable by hackers.
- The extent to which there is an understanding in the banking sector that software vulnerabilities found in in-house-developed software could also be exploited by hackers.
- The extent to which there is an understanding in the banking sector that software vulnerabilities and accompanying exploits can be purchased on the hacker marketplace.

**IT risk**
- The extent to which the banking sector realises that new technologies, such as cloud computing, bring new risks which need to be considered before taking up such services.

### 3.8.6 Global interconnectedness of networks

Another important factor that contributes to successful hacker attempts is the interconnectedness of networks, which was also discussed in section 2.4.

Hackers can gain access to systems situated anywhere across the globe (Kovacich, 1998:132) with the Internet being the gateway into many organisations’ systems. Should the hacker successfully gain access to an organisation via a vulnerable access point, he or she could propagate himself across the LAN or WAN environment of the organisation itself (Day, 2003:136). This risk is increasing exponentially as free wireless networks are available at many coffee shops, cyber cafés, university campuses, hotels and airports. By using these free access points hackers can remain anonymous or prey on other unsuspecting users who are also making use of the free access points (Gallegos, 2004:19; Pickard, 2007:337).

Hackers can also target an organisation’s network specifically, such as attacking critical network routers, which may fail under the unusually high volume of network traffic and subsequently cause total communication failure in the organisation’s network (Skoudis & Liston, 2006:517-518; Khare, 2006:167).

The Internet enables the banking industry to explore new revenue streams, such as Internet banking. Alongside the numerous benefits, there are also numerous weaknesses and threats. In South Africa, there has been an increase in the number of phishing attacks against unsuspecting Internet banking users. The interception of credit card or bank details of clients seems to be a popular form of cybercrime in South Africa. For an eight-month period starting February 2009, the Nelson Mandela Bay commercial crimes unit alone
Chapter 3

reported 13 cases, with reported losses totalling R1.2 million (Sonjica, 2009). Phishing attacks can be very sophisticated and personalised, such as the example of Standard Bank employees who received a fraudulent email from their manager notifying them of an “account upgrade”. A few employees divulged their account details on a fraudulent website and suffered financial losses (Meyer, 2010:7). In another phishing-related incident, Absa Bank stopped credit card transactions processed via the utility bill payments site, EasyPay, after it was discovered that one in three transactions were fraudulent. Fraudsters were buying airtime and prepaid electricity for resale at a profit. The exact extent of the fraud is unknown, but Absa has reversed at least R500 000 worth of transactions. The South African Banking Risk Information Centre (hereafter Sabric) has warned the public of the increase in phishing emails (Mawson, 2011a). EasyPay responded to the incident by stating that their website was not responsible for the fraud. They were simply processing the transactions. They blame the “inherent risks of the current banking system” and “security loopholes of the national payment system” as the cause of this fraud (Net1 U.E.P.S. Technologies, 2011). Even though the clients are responsible for protecting their banking details, increasingly banks are expected to protect their clients against fraudulent transactions.

Advances in cell phone technology have increased the uptake of mobile banking. Users require real-time access to and control over their banking information. Mobile banking also reaches unexplored client segments, who might not have access to PCs and the Internet. Both the fixed-line and wireless technologies will integrate seamlessly to provide customers with even more product offerings (TowerGroup, 2009).

New technologies relying on the Internet, such as voice over IP (hereafter VoIP), will decrease telecommunication costs, but at the same time bring new challenges. Threats associated with VoIP include concerns related to the confidentiality of VoIP data (intercepted by hackers), hackers masquerading as a legitimate caller (also known as “spoofing”) and receiving spam over Internet telephony (hereafter SPIT), which involves receiving pre-recorded unsolicited calls (DeSantis, 2008:3-4). This is possible due to the use of already existing networking technologies, which often entail large-scale deployments in organisations (Drew & Gallon, 2003:3).

**Thematological research questions**

Based on the literature review above, the following thematological research questions can be defined:

**IT risk**

- Whether the banking sector understands the risks associated with new Internet technologies and
solutions.

- The extent to which banking clients are protected against phishing attacks.

**Hacker threat**

- The extent to which there is an understanding that hackers can attack the banking sector from remote destinations, possibly gaining entry into a bank’s inner network.
- Whether the banking sector understands how quickly hackers can become familiar with new and emerging technologies.

### 3.8.7 The human factor

The last important factor to consider under the heading of weaknesses that facilitate successful hacking attempts is one far removed from technology – the human element and human fallibility, perhaps most aptly described by Albert Einstein (Whitman & Mattord, 2008:315), albeit in a context far removed from hacking:

> Only two things are infinite, the universe and human stupidity, and I’m not sure about the former.

When considering the human element in the context of the threat of hacking, there are a number of nuances to consider:

- Firstly, the formulation of IT policies and procedures to enforce appropriate behaviour is of consideration. McGhee (2008:38) writes that employees are often unfamiliar with the organisation’s IT policies. He added that weakly written policies could also lead to human error (McGhee, 2008:48). Many of the issues discussed here can be regulated via IT policies. Failure to do so leads to uninformed users, exposing the organisation to hacking threats. Failure to follow defined procedures could also increase the hacker threat. Fried (2006:411-412) emphasises that even when an organisation has appropriate controls in place to identify hacker attacks, employees tend to ignore the controls which are intended to identify the hacker activity, such as reviewing access logs.

- Secondly, weak security practices are a major contributor to successful hacking attempts (Beaver, 2004:11). Even with the most sophisticated information security practices, humans will find a way of circumventing them (Day, 2003:132). For example, employees often write down their complex passwords on a piece of paper and store it in their drawers. Alternatively, system administrators could make use of a vulnerable file transfer protocol (hereafter FTP) service for file transfers, simply because it is convenient to use. On another level, many hackers make use of social engineering...
techniques to obtain privileged access by for example phoning an IT helpdesk and impersonating a legitimate user (Krone, 2005b; Harris, et al. 2005:16; Fried, 2006:411-412).

• Thirdly, skills shortages or overworked staff also play a role in facilitating hacker attacks. For example, when it comes to the secure configuration of systems, which is a complex task, the system administrator may not have the knowhow to successfully complete this task, or he or she may not complete the task because he or she is overburdened with remedial support tasks, so effectively neglecting his duties, leaving the system vulnerable to attack (Schell & Martin, 2004:85). Weaknesses associated with logical access controls discussed in section 3.8.4 should also be considered here. For example, employees might store confidential data on a USB storage device, while at the same time using it to store personal data such as computer games and photos. The employee could place this data at risk when sharing the USB devices with friends or putting the USB at a risk of theft by simply carrying it around outside of the boundaries of the organisation. A similar risk exists for other mobile devices, such as PDAs that might be misplaced (McGhee, 2008:36-37).

• Next, vendors and third parties interacting with organisations could also be a threat. The intentional or accidental actions of third parties may expose the organisation to hacker threats. They are sometimes inadvertently given full access to production systems, without assessing their integrity or motives. They might inadvertently use laptops and software, not necessarily approved by the organisation, which may contain hacker software or malware. In the process they might circumvent the organisation’s information security policies. Their own systems might be insecure, exposing the organisation to malware. Vendors could create backdoors, unbeknown to the system owner, which may be used to access the system remotely. The backdoors may be discovered by hackers, who then use it to bypass perimeter security (Dubin, 2007). Of course, an insider could collude with a third party, significantly increasing the risk of unauthorised access.

• Another consideration is the clients of organisations, who could also fall prey to hacker attacks. The typical online banking customer in fact knows very little about the technical aspects of online banking security. Even when banks make security recommendations, such as advising a client to install anti-virus and firewall software, clients might not have the technical knowledge to do so. Clients might also fail in
selecting secure passwords or regularly changing their passwords (Mannan & Van Oorschot, 2008:1, 10, 11).

- Lastly, clients might lack the necessary awareness of hacking and cybercrime threats. This could lead to poor personal information security practices. Similar to employees, customers could also write down their pin and password, letting it fall into the hands of a fraudster. Clients may inadvertently answer an illegitimate e-mail from a cybercrime syndicate, divulging their logon details. Alternatively, they could make use of public access points (such as Internet cafés) to perform Internet banking activities, where keyloggers could capture their credentials (Sonjica, 2009). Clients may simply be unable to distinguish between legitimate websites and web-browser security features (Dhamija, Tygar & Hearst, 2006:581, 589). All of these examples are avoidable; however, the reality is that human fallibility leads to actions of this nature.

### Thematological research questions

Based on the literature review above, the following thematological research questions can be defined:

**Business risk**
- The extent to which there is an appreciation, particularly in the banking sector, that poor human security practices increase the risk of hacking.
- Whether the public should hold the banking sector responsible for protecting it against hacker attacks.

**IT risk**
- Whether the public is aware of the threats associated with the use of the Internet and related services and technologies, in particular from a banking product perspective.

**Hacker threat**
- Whether employees in the banking sector are aware of the threats posed by insiders.

**Hacking response**
- Whether there are written procedures and formal policies in place in the banking sector to keep basic security procedures such as securing passwords at the forefront of employees' minds.
- The extent of procedures and steps taken to constantly alert Internet users, particularly in the banking sector, of risks such as phishing.
- The extent to which management accepts responsibility for protecting and educating online banking clients to be cautious of phishing and similar attacks.
- Whether online banking clients understand the role they play in securing transactions conducted on the Internet.
- Whether the public using banking products has the knowledge to protect itself against hacker attacks.

### 3.8.8 Conclusion

The discussion above has presented a number of factors that contribute to successful
hacking incidents. The general availability of information, both commercially and publicly, allows hackers to learn the techniques required to hack into systems. The affordability and ease of use of PCs and Internet access have contributed to the growing threat of hackers. Risks associated with physical access to an organisation’s premises, coupled with the use of social engineering techniques, have increased the risk of unauthorised access by hackers, while vulnerabilities in software and hardware also play an important role. The threat associated with new technology such as USB storage devices, cellular telephones, smart phones, PDAs and Blackberry devices, which allows for the removal of critical and confidential corporate data outside of the physical security measures of the organisation, also needs to be considered. If the human factor, which blends with the threats associated with today’s technology, is factored in, it is clear that the threat of hacker attacks can loom large.

In response to the threat posed by hackers, the vulnerabilities and weaknesses discussed in this section need to be addressed. This requires a multi-level response, covering not only the known weaknesses, but also taking on the challenge of addressing the unknown. Responses to the hacker threat will be further explored in chapters 5 and 6.

Given the range of weaknesses that contributes to hacker attacks, it is to be expected that hackers use a range of different techniques to ply their trade.

3.9 HACKER TECHNIQUES

In plying his trade, a hacker will make use of various techniques, which are well described in the literature. An important consideration at this point of the study is to consider the size and complexity of the organisation. The choice of some hacker techniques could be linked to a particular piece of technology. Complex or expensive types of technologies might be absent at smaller-sized organisations. Consequently, the associated hacker technique will not be an option. In contrast, as will be discussed, social engineering might be successful for all types and sizes of organisations (if they have systems or networks to target).

As the purpose of the presentation of the techniques commonly used by hackers is to better understand the nature of hacking, a number of sources related to hacking specifically and information security in general will be discussed to provide an overview of the myriad of attack techniques used by hackers. With this knowledge, a deeper response to the hacker threat and how the attack techniques integrate with the hacker methodology discussed in
section 3.6 can be defined. It is also important to note that not all hacker techniques and
attack types are technical in nature, which implies that some hacker techniques might be
easier to master than others.

3.9.1 General hacker techniques from selected sources on hacking

There are so many varying hacker techniques and attacks available that they have become
the topic of entire textbooks. Some textbooks are very technical, explaining how to write
exploit code, such as Harris, et al. (2005) and Oppleman, Friedrichs and Watson (2005). It is
not the objective of this thesis to discuss the technical details of hacker techniques, but
rather the general principle. Although several sources on hacking have been consulted as
part of this study, for the purpose of this discussion on hacker techniques, two sources have
been selected (one textbook and one journal article), which, based on the author’s
experience, provide a basic non-technical and well-structured overview of hacker
techniques.

3.9.1.1 General hacker techniques by Skoudis and Liston

Skoudis, a lecturer of ethical hacking courses (at the industry-leading SANS Institute), a
regular speaker at information security and hacking conferences, and author of several
books (Bradley, 2009) discusses numerous attack techniques in his book titled Counter
Hack Reloaded (co-authored by Liston), logically grouping the attack types under the
headings of each hacker methodology phase:

- Phase 1: Reconnaissance:
  - Low-technology reconnaissance: This includes attacks such as social
    engineering, caller ID spoofing, physical break-in and dumpster diving used
during the reconnaissance phase of the hacker methodology, as discussed in
section 3.6. Caller ID spoofing involves making a call to an organisation’s voice
mail administrator, masquerading as a new user and requesting voice mail
service. The hacker will then leave a message on an unsuspecting user’s voice
mail, requesting sensitive information (Skoudis & Liston, 2006:184, 186-187).
  Other social engineering attack techniques will be discussed in section 3.9.4.
  - Searching the Web: Hackers can obtain a significant amount of public information
on a particular organisation by using search engines and “whois databases”.
Firstly, hackers use complex search queries on popular search engines, such as
Google, to obtain detailed information about the company being targeted by the
hacker. The search engine queries could also return electronic documents, which
may contain user names and passwords. In fact, there is an entire hacking discipline around the use of search engines, called “Google Hacking” (Skoudis & Liston, 2006:196, 204). The second aspect to be discussed is a “whois database”. Whois databases contain data related to the assignment of domain names, individual contacts and Internet Protocol (hereafter IP) addresses (Skoudis & Liston, 2006:212). The domain name ensures that an organisation has a unique name, which is accessible when you type in a friendly URL, such as www.uj.ac.za. This information is used by a hacker to plan an attack, such as attacking the websites of subsidiaries rather than the organisation’s primary website, which might be more secure.

- Interrogating DNS: The domain name system (hereafter DNS) is a hierarchical database distributed around the world, which stores domain names, related IP addresses and mail server information. Whenever a user tries to access a particular website, the user’s browser sends a request to the DNS, which in turn resolves the friendly URL, by returning an IP address of the website to be visited. A hacker would use DNS to obtain IP address ranges and mail service information, which could be used to plan an attack (Skoudis & Liston, 2006:220-222).

- Phase 2: Scanning:
  - Wardriving: The process of finding unsecured wireless access points, providing the hacker free Internet access or access to a corporate wireless LAN (Skoudis & Liston, 2006:240) as discussed in section 3.8.3.3.
  - Wardialling: The process of finding unsecured modems connected to an organisation’s network or systems. A wardialling software tool is often used to dial thousands of telephone numbers consecutively (Skoudis & Liston, 2006:252) during the scanning phase of the hacker methodology, as discussed in section 3.6.
  - Network mapping: Involves the process of finding additional targets to attack and discovering the network topology. A hacker would carry out ping scans on entire network address ranges, hoping to discover active listening servers on the network. Another technique used is “traceroute”, which discovers the path or route network traffic would take to get to its destination (Skoudis & Liston, 2006:261-262). This is also used during the scanning phase of the hacker methodology, as discussed in section 3.6.
  - Port scanning: Once an attacker has discovered a possible target, the next step would be to discover open ports on the target. The open ports discovered will
provide clues as to the type of services available on the target, such as FTP, e-mail and telnet (a protocol used to connect to remote machines). Once this has been established, further inferences could be made regarding the operating system being used on the target. Nmap is an example of a popular multi-featured port scanning tool (Skoudis & Liston, 2006:268-269) used during the scanning phase of the hacker methodology, as discussed in section 3.6.

- **Vulnerability-scanning:** This involves the use of tools that automate the processes of discovering common configuration errors, configuration weaknesses and known system vulnerabilities of the target. A vulnerability scanning tool, such as Nessus, has a vulnerability database which is updated regularly by its developers and various other configuration options and reporting options, to customise each scan (Skoudis & Liston, 2006:308-310). This technique will be used during the scanning phase of the hacker methodology, as discussed in section 3.6.

- **IDS and Intrusion Prevention System (IPS) evasion:** IDS and IPS are designed to identify or block hacker scanning and attack activity. IDS and IPS evasion involves obfuscating the scanning and attack activity network traffic, to avoid detection by the IDS and IPS (Skoudis & Liston, 2006:320). This tends to be a complex attack technique.

- **Phase 3, Type 1: Gaining access using application and operating system attacks:**
  - **Buffer overflow exploits:** This attack technique targets buffer overflow vulnerabilities, which involves the hacker sending more data to a vulnerable application or operating system than it was designed to handle. This results in unintended consequences, such as changing the flow of the program or variables (Skoudis & Liston, 2006:342). This might allow the hacker to access restricted application functionality.
  
  - **Password attacks:** Password attacks involve either guessing a password, by using well-known default passwords (as discussed in section 3.8.4) or by using password attack tools, which generate thousands of passwords, based on password syntax rules or by using dictionaries. A distinction can be made between passive and active password attacks. Passive attacks involve obtaining the password hashes and running software which generates similar hashes, until a match is found. Active attacks involve sending sequential or random passwords to the application requesting authentication details, until a valid password is found (Skoudis & Liston, 2006:378-380, 383). Also refer to section 3.9.2 for a discussion of different types of password attacks.

  - **Web application attacks:** There are numerous web application attack techniques
available that exploit the weaknesses in web-application designs and technologies. Skoudis and Liston discuss only a few, such as “account harvesting”, which involves determining the authentication details of a valid user by analysing the error messages returned by a web application (Skoudis & Liston, 2006:406-407). Other web application attacks are discussed in section 3.9.3.

- Phase 3, Type 2: Gaining access using network attacks:
  - **Sniffing:** A “sniffer” is a program which captures data passing the local PC connected to the network. A hacker could capture a wide variety of data, such as the content of e-mails, passwords sent in clear text or even application or transaction data, compromising user confidentiality in the process. There are numerous tools available to facilitate networking sniffing, such as Wireshark and Dsniff (Skoudis & Liston, 2006:439-442).
  - **IP address spoofing:** This technique is used where the attacker would want to remain anonymous and avoid being traced, or where a particular application’s response can be redirected to the attacker, by masquerading as the original target (Skoudis & Liston, 2006:470-471). At a basic level, it involves changing the hacker’s IP address and manipulating the route of the network traffic.
  - **Session hijacking:** This technique involves taking over an existing application session established between two systems. By sniffing the network traffic and spoofing the originating IP address, the target system will establish the session with the hacker’s system, believing that it is a valid session (Skoudis & Liston, 2006:482-483). This technique is similar to Address Resolution Protocol (hereafter ARP) spoofing, when fake ARP messages are sent to a LAN (Cole, 2002:498), and is considered technical in nature.

- Phase 3, Type 3: DoS attacks:
  - **Stopping services:** This attack could be done on a local machine or remotely. It involves stopping a system process or application by suspending the system process, reconfiguring the system or even forcing or “crashing” the system process to stop (Skoudis & Liston, 2006:515, 518), compromising the availability of the organisation’s systems.
  - **Exhausting resources:** This attack can be done locally or remotely. It involves exhausting the resources on a system through duplicating system processing, filling up the file system with erroneous data or flooding the communication link with erroneous network traffic (Skoudis & Liston, 2006:517, 523).
Phase 4: Maintaining access: Trojans, backdoors and rootkits:

- **Trojans**: Trojan horse software is programs that appear to have a legitimate purpose; however, they hide a malicious component which is executed either remotely or activated under certain conditions (Skoudis & Liston, 2006:548; Decloedt & Van Heerden, 2010:8). This is used during the “maintaining access” phase of the hacker methodology, as discussed in section 3.6.

- **Backdoors**: Backdoor software allows a hacker to bypass the normal system security and enter the system via an alternative access mechanism installed by the hacker. “Botnets”, a concept which refers to a number of systems controlled by a hacker to orchestrate attacks against a single target, all fall under the backdoors category (Skoudis & Liston, 2006:548-549, 569; Decloedt & Van Heerden, 2010:7). This is used during the maintaining access phase of the hacker methodology, as discussed in section 3.6.

- **Rootkits**: Hackers install rootkits on systems to replace existing programs in the operating system, to allow easy access to the system or to hide from detection. The rootkit might also add additional functionality, such as adding a sniffer to existing system tools (Skoudis & Liston, 2006:588, 592; Decloedt & Van Heerden, 2010:7). The development of rootkits is highly technical and complex in nature. They are used during the maintaining access phase of the hacker methodology, as discussed in section 3.6.

Phase 5: Covering tracks and hiding:

- **Altering event logs**: To avoid detection by the system administrator, hackers might have to clear entries in the system log files. The type of system log entries includes user logins, traces of software installation and privilege escalation (Skoudis & Liston, 2006:628-629). This is used during the cleaning-up phase of the hacker methodology, as discussed in section 3.6.

- **Hidden files and directories**: A hacker could hide his activity on a system by creating hidden directories or files. The syntax format of the hidden directories and files is such that they cannot be easily spotted by normal users or administrators (Skoudis & Liston, 2006:641).

- **Covert channels**: To ensure that hacker activity remains hidden, including the communication channel with the remote system, a hacker would use covert channels and “tunnelling” techniques. Tunnelling involves carrying one communications protocol within another (Skoudis & Liston, 2006:647, 649).
3.9.1.2 General hacker techniques by Harding

A second source to consider is an article published in the Institute of Internal Auditor’s (hereafter IIA) IT audit e-journal, written by Harding, who has provided advice on preventing hacker attacks in a professional capacity and worked as a security design engineer for most of his career. He warns that hackers are often very patient by nature and would take their time to collect enough information from the target, before launching an attack. Based on his security design engineering experience, he provides a broad overview of types of hacker attacks (Harding, 2002):

- **Buffer overflows** involve exploiting software vulnerabilities in the target. The target PC or server will accept some form of input, for example, an FTP service waiting for FTP traffic. The hacker would send a piece of code as input. When the piece of code is executed, the target performs an illegal action, such as granting the hacker full access to the host machine. The design and development of this kind of attack is technical in nature.

- **Environment variables** are related to operating system programs, which will react to environmental variables, and could allow erroneous data and perform illegal program functions, such as granting access to the system. This type of attack is similar to a buffer overflow.

- **Race conditions** occur when a hacker changes code between valid program steps, in order to manipulate the outcome of program steps.

- **Backdoors, rootkits, and Trojans** are installed once access to the target system has been obtained. Applications of this nature might allow the hacker to gain unrestricted access to the target. They are used during the maintaining access phase of the hacker methodology, as discussed in section 3.6.

- **Network sniffing** is accomplished through the use of specialised applications, which can read the network traffic intended for other recipients. It is used in particular to discover usernames and passwords sent in clear text across the network.

- **Password guessing** can be done manually or through automated applications. Manual password guessing involves simply randomly guessing the password. Automated hacker tools are available to “brute-force” a password, by using a dictionary wordlist or by using character and numeric combinations. This technique is used either during the scanning or attack phase of the hacker methodology, as discussed in section 3.6, and relates to weaknesses discussed in section 3.8.4.

- **Social engineering** is considered by Harding as the most powerful yet least technical of all attack techniques. The classic example of social engineering is the hacker
impersonating a user and calling a helpdesk to ask for a password reset, as is typically done during the reconnaissance phase of the hacker methodology, as discussed in section 3.6.

- **Protocol vulnerabilities**, such as security protocols SSL and secure shell (hereafter SSH), Transmission Control Protocol / Internet Protocol (hereafter TCP/IP) and DNS are examples of protocols, which, depending on the software release, may contain vulnerabilities which are exploited by hackers.

- **Default or insecure configuration** refers to basic configuration errors when setting up a server or router, such as not changing the default password. These would be exploited by hackers.

- **Bad parameter parsing** (syntactic analysis) involves, for example, input validation weaknesses in the password authentication program, which allows the hacker to enter a password combined with another piece of text, which contains a structured query language (hereafter SQL) statement. When executed, the SQL statement is also executed, which returns confidential information from the database where the passwords are stored.

- **Unauthorised remote access** is achieved when wireless and dial-up modems are poorly configured, allowing the hacker to enter the network without being authenticated.

Not surprisingly, hacker techniques are often used during the attack phase of the hacker methodology (as discussed in section 3.6). Buffer overflows, password guessing and network sniffing have all been mentioned by Skoudis and Liston, and Harding as attack techniques used to gain unauthorised system access. The two sources referenced also provide an indication of the wide variety of techniques, which are often technical in nature.

### 3.9.2 Hacker techniques defined in ethical hacking qualifications

Another area where hacker techniques are defined is found in ethical hacking qualifications. A well-known and reputable organisation which offers ethical hacking and information security courses is the SANS Institute. The institute is based in Maryland, USA, yet does offer extensive training through online classes and self-study. The organisation offers four audit-related courses. One of these courses focuses specifically on hacker techniques, exploits and incident handling (Pan, 2007:259). Some of the attack types covered in this course include network-level attacks, such as session hijacking, man-in-the-middle attacks (eavesdropping on communication between two parties) and passive sniffing. Operating
system and application-level attacks are also covered, and include attacks such as buffer overflow and format string attacks (The SANS Institute, 2009).

The courseware for the Certified Ethical Hacker (hereafter CEH) qualification offered by the EC-Council distinguishes between four attack types: operating system, application level, shrink wrap code and misconfiguration attacks. Firstly, operating system attacks are possible due to the complexity of operating systems and the large number of services and open ports made available by operating systems. Secondly, application-level attacks are successful due to poor software development practices and the resulting coding and security weaknesses. In the third attack type, hackers make use of code and script available by default in installed applications to carry out their attacks. This is referred to as shrink wrap code attacks. Lastly, the misconfiguration of applications, systems and operating systems allows hackers to exploit weak or ill-configured services and software (EC-Council, 2008a:21-22, 23-26).

One of the most frequently attacked vulnerabilities is weaknesses in logical access controls, in particular password weaknesses. Four types of password attacks can be distinguished (EC-Council, 2008b:793):

- **Passive online attacks.** “Wire sniffing” is a form of passive online password attack and involves the use of sniffer software to obtain user credentials. This kind of attack works only within a hub-network, where all the traffic in the network is routed to all PCs. Most networks today are either switched or bridged networks, which voids the use of a sniffer (EC-Council, 2008b:794).

- **Active online attacks.** This involves the process of guessing a user’s password. Often, automated password attack tools are used, which pass thousands of words taken from custom-made dictionaries through to the authentication mechanism (EC-Council, 2008b:796).

- **Offline attacks.** This is only possible if the hacker managed to obtain the password file containing the encrypted passwords. The hacker would use dictionary attacks (random words) or brute force attacks, where every single combination of character and numeric value is used to recreate the encrypted password, until a match is found (Skoudis & Liston, 2006:384; EC-Council, 2008b:797, 799).

- **Non-electronic attacks.** Non-electronic attacks use social engineering techniques to obtain passwords. Shoulder surfing is an example: here the hacker would observe the user typing his password, without being noticed (EC-Council, 2008b:806). Once valid credentials have been obtained, hackers will access the operating system or application and try to create fictitious users, which can then be used to masquerade as
a legitimate user (Cornett, Grewal, Long, Millier & Williams, 2009:114). A hacker might use this access to commit fraud (by processing transactions as a legitimate user) or steal valuable data.

3.9.3 Hacker techniques for web application attacks

The third area to consider is hacker techniques used to attack web applications. This tends to be a unique area with distinct hacker attack techniques. But organisations are increasingly making use of the Internet and web-enabled applications, which are easily accessible by customers and hackers alike. There are numerous examples of web applications, including shopping, social networking, banking, search engines, auctions, casinos, blogs, webmail and encyclopaedic sources (Stuttard & Pinto, 2008:3-4). Entire books have been written on the subject of web application hacking, such as by Scambray, Shema and Sima (2006) as part of the popular Hacking Exposed series, Palmer (2007) and Stuttard and Pinto (2008). The attack complexity ranges from the very straightforward to the complex. An example of a simple attack is to obtain the web-master or administrator password, which allows the hacker to gain access to the web-server content (EC-Council, 2008b:1627-1630).

Stuttard and Pinto provide a comprehensive account of web application attacks. Some of the key attack techniques covered are listed next:

- **Bypassing client-side controls** involves manipulating hidden form fields (data not displayed to the user), or changing the details contained in Hypertext Transfer Protocol (hereafter HTTP) cookies (small text files containing user- and session-specific details), or manipulating URL parameters (changing the values passed by the URL). It is also possible to manipulate captured user data on HTML forms to cause unexpected behaviour (Stuttard & Pinto, 2008:96, 99, 106).

- **Web authentication mechanisms**: Many web applications make use of an authentication mechanism to restrict access to legitimate users. There are numerous ways of implementing authentication in web applications, which in turn can be exploited. Examples of web application authentication mechanisms include weak passwords and verbose error messages, which provide clues as to the particular portion of the authentication mechanism which failed (Stuttard & Pinto, 2008:135, 139).

- **Attack session management** is a sophisticated attack technique that involves manipulating web application session functionality. Sessions are established by web applications to uniquely identify a particular user and ensure that the session remains active for the period of the transaction. Session tokens could contain, for example, user
credentials, encoded with simple encryption. When decrypted by a hacker, the credentials could be used to access the web application as a valid user. Tokens could be obtained by capturing them from the network with sniffer software (such as Wireshark). Session tokens are also sometimes stored in web server or user browser logs (Stuttard & Pinto, 2008:175, 180, 196).

- **Attacking access control** is one of the basic attack vectors a hacker could consider. Web server resources, such as directories and files, might be unprotected. The access control functionality might have an inherent weakness, such as simply changing the URL parameters to the desired value to allow access (Stuttard & Pinto, 2008:219, 223).

- **Injecting code**: There are a significant number of web attacks which make use of injecting code. Code could be injected into the interpreted language, such as commands executed at the operating system command line, which discloses more operating system information than it should have. Web applications often make use of databases. SQL is often used to access the information in the database. By not sanitising and formatting the data passed via SQL queries, hackers could manipulate the SQL queries. The end result of manipulating the SQL queries could range from obtaining classified data from the database to bypassing security. This is referred to as “SQL injection”. Code injection could also be applied to web scripting languages, Simple Object Access Protocol (hereafter SOAP), XML Path Language (hereafter XPath), Simple Mail Transfer Protocol (hereafter SMTP) and Lightweight Directory Access Protocol (hereafter LDAP) (Stuttard & Pinto, 2008:238, 241, 243, 307, 313, 316, 321, 326), which, due to the technical nature of these attacks, will not be discussed in detail in this thesis.

- **Exploiting path traversal** is an attack technique made possible due to the extensive use of directories and files on web servers. It involves manipulating the URLs to gain access to restricted web server files and directories (Stuttard & Pinto, 2008:334).

- **Attacking application logic** involves exploiting the weaknesses in the logic of the web application. Attacks of this nature vary greatly and depend on the intuition of the attacker to discover the weaknesses (Stuttard & Pinto, 2008:350).

- **Attacking other users** involves making use of the web application to attack other users of the same web application. Cross-site scripting (hereafter XSS) is the most common form of attack against other users. It involves the insertion of code, which, when executed, creates web content, with numerous side effects, such as misleading the user into divulging sensitive information or taking over the user’s session. There are also a number of other attacks falling under this category, which will not be discussed...
in detail, due to the technical nature of the attacks, such as frame injection, request forgery, JSON hijacking, session fixation, attacking ActiveX controls and local privacy attacks (Stuttard & Pinto, 2008:375, 376, 380, 438, 440, 446, 450, 454, 458).

- *Exploiting information disclosure* involves interpreting the error messages returned by web applications, which might point out the programming language being used, or provide information related to the server or database. It is also possible that a web application might simply display sensitive data, such as user profiles or log files (Stuttard & Pinto, 2008:505, 506, 509, 513).

Web application input fields often lack input validation, such as data types and data ranges. A hacker would manipulate these fields in order to pass invalid input to the web-application, causing it to perform abnormal or illegal actions (Khare, 2006:172). Input fields often use SQL commands to accept input. This could lead to the alteration of data or transactions, or add a fictitious user to the database, or return the results of an unauthorised data query from the database (Khare, 2006:173; Skoudis & Liston, 2006:423-424).

Many of the attack techniques listed above can be used to perform web-defacement, such as XSS and using path traversal to get to modifiable website files (Palmer, 2007:193; Stuttard & Pinto, 2008:344, 392), leading to the unavailability of these websites.

### 3.9.4 Hacking techniques of a non-technical nature

As discussed at the start of section 3.9, not all hacker techniques are technical in nature. Macleod points out that insider hacker attacks may be conducted by using default lists of administrator or root passwords (Macleod, 2007:47). Graves, author of review guides used for the internationally recognised CEH qualification, discusses various social engineering techniques which are non-technical in nature that could be used by a hacker (Graves, 2007:32-33, 78):

- **Impersonating an employee or valid user**: by pretending to be an employee of an organisation and obtaining “valid” access to the premises.
- **Posing as an important user**: threatening more junior staff to grant him immediate access to a sensitive system.
- **Using a third person**: the hacker falsely claims that he or she has the authority of an authorised third person.
- **Calling technical support**: making the helpdesk or IT support believe that the hacker is a legitimate user and subsequently granting the hacker unauthorised access.
• **Shoulder surfing** involves observing user credentials being entered while a valid user is doing it.

• **Dumpster diving**, as defined earlier in section 3.6.

Similar social engineering hacking techniques are discussed by Okenyi and Owens (2007:304) and Frangopoulos (2007:65, 70, 76), such as shoulder surfing, phishing, dumpster diving, and impersonation. Graves also points out that breaching the physical security of an organisation, a non-technical attack technique, could result in unauthorised access to the organisation’s IT systems and could lead to theft of data or damage to systems (Graves, 2007:171). Many of these attack techniques are used either to gather information about the organisation or to attack the organisation during the corresponding hacker methodology phases.

3.9.5 **Hacker techniques defined by the IT Governance Institute**

Given the focus of this thesis on corporate governance and IT governance, hacker techniques listed by related sources need to be considered. Chapter 11 of the CoBIT Security Baseline Information Security Survival Kit provides a summary of technical security risks (and associated threats) encountered in today’s technologically advanced business world. The threat agents include hackers, fraudsters, criminals and terrorists (ITGI, 2007c:12). This guideline issued by the ITGI provides guidance to users, management, executives and board members to assist them in being aware of the most significant IT risks. It also indicates that it is not only hackers who are using hacker techniques, but also other criminal agents. The opposite is also true in that hackers may use ordinary crime tactics, such as theft, to achieve their goal. The following are examples of crimes which may be executed by criminals in general and hackers alike, as listed in Table 3.1 (ITGI, 2007c:37-40):

| Table 3.1 Cybercrime and hacker techniques (ITGI, 2007c:37-40) |
|---------------------------------|---------------------------------|
| Trojan horse programs.         | Hidden file extensions.         |
| Back door and remote administration programs. | Chat clients.                 |
| Intermediary.                  | Identity theft.                |
| Unprotected Windows networking shares. | Tunnelling.                  |
| E-mail spoofing.               | Zombies.                       |
| Inappropriate or accidental data disclosure. | Spyware.                     |
| Physical theft.                | Phishing.                      |
| E-mail-borne viruses.          | Mobile code.                   |
| Cross-site scripting.          |                                |
3.9.6 Other general hacker techniques

As will be discussed in section 3.10, the application of malware is typically classified as cybercrime. Yet hackers often use malware to deliver backdoors or software which can be used for nefarious hacker activity (Bahadur, et al. 2002:396). The effect of malware could be devastating. In February 2003, the Slammer worm infected 75 000 servers, bringing down 13 000 of the Bank of America’s ATM machines. The worm also caused airline delays and publishing problems at media outlets. The Sobig.F virus infected millions of PCs and resulted in 300 million infected e-mails being sent out in its first week (O’Neil, 2006:228). SPAM email (unsolicited or “junk” email) can also be used as a delivery mechanism for viruses (Geissler, 2004:106). Trojans are becoming increasingly more sophisticated, stealing user credentials and circumventing application controls implemented by organisations (Maor, 2010:10). Malware as a hacker technique should not be ignored. Viruses could affect many components of computers, such as the general hardware, operating system configuration, basic input-output system (hereafter BIOS) and peripherals attached to the PC, such as causing a flickering of the monitor. Viruses can accidentally or intentionally alter files and data stored on a PC or server. It is clear that a large-scale infection could cause major disruption, wasting valuable resource capacity and time (EC-Council, 2008b:1238-1246).

It should be noted that hackers would not necessarily be knowledgeable in all of the attack techniques presented in this thesis; they would specialise in a number of them, or learn new techniques when faced with a new challenging target. Given the broad range of hacker techniques, a security breach can be a significant threat to the integrity of an organisation’s data and other factors, such as its reputation. Hackers often leave behind a trail of destruction, accidentally or intentionally altering or deleting confidential or operational data without understanding the implications thereof (Yar, 2006:28).

From the literature discussed, it is evident that some hacker techniques are technical in nature, while others take advantage of the human factor. Hackers could use any one or combination of these techniques to break into a target system. The objective is mostly to gain unauthorised access to a system, where after actions can be performed as a legitimate user. Although a hacker might enjoy using a sophisticated attack technique to gain entry into a target network, social engineering might be an easier option to produce the same results.
### Thematological research questions

Based on the literature review above, the following thematological research questions can be defined:

**Business risk**
- Whether the banking sector understands how the different hacker attacks could affect its business operations.

**Hacker threat**
- Whether the banking sector has an appreciation for the range of hacker techniques that could be used, including technical, human and physical techniques.
- The extent to which there is an understanding in the banking sector that hacker attacks vary in complexity, ranging from simple to highly technical.
- Whether there is a realisation in the banking sector that unsophisticated hacker attacks could be even more successful than technical hacker attacks.

**Hacking response**
- The extent to which the banking sector has the capacity and expertise to deal with both technical and non-technical hacker attacks.

### 3.10 HACKING: A TYPE OF CYBERCRIME

Although the wider field of cybercrime falls beyond the scope of this thesis, it is important to provide a brief overview of cybercrime and its relationship with hacking, as it will assist in understanding the nature of hacking. This will also ensure that a broad enough response to the hacking threat is defined.

Cybercrime is regarded as a growing threat that could be of such significance that it could have a debilitating effect on the total economy of a country (Aginam, 2009). There are varying definitions of the concept cybercrime and the exact scope of the crimes associated with it. It has been defined in the literature as crimes committed with the use of PCs and other IT devices (Gordon & Ford, 2006:14). It has also been defined as crimes which are not only facilitated by, but also committed against, computers as the target (Pati, 2003). It has also been described as the duplication of crimes, which usually take place in the real world, but that now take place in the virtual world (Labuschagne, as quoted by Venter, 2005). All of the aforementioned definitions point to the fact that computers or similar IT equipment are the common denominator in all these crimes. Moreover, it is clear that PCs can be both the target and the tool used to commit cybercrimes.

Cybercrime is regarded as a profitable, low risk type of crime, with losses reported by researchers varying, such as the example of 41 hackers arrested by Brazilian police in
February 2007, who used Trojans to steal $4.74 million from bank accounts (Kaspersky, 2008:2). On the other side of the spectrum, a report by the malware security company McAfee reported intellectual property losses for 2008 among a 1000 large organisations amounting to $559 million. An industrial espionage case is another example of a cybercrime incident reported, where sensitive data was to be sold for $139 million (McAfee, Inc. 2009:7, 19). It was reported by Reuters that global cybercrime losses have reached the $100 billion mark (Maclean, 2009). In its National Security Strategy report, issued in October 2010, the United Kingdom (hereafter UK) coalition government identified cybercrime as one of the biggest threats to UK national security. It has been compared to other threats, such as terrorism, natural disasters and military crises (Crown, 2010:27). The report does not see cybercrime as a mere risk, but recognises it as a daily occurrence, resulting in the loss of commercial and government information, and leading to identity and intellectual property theft (Crown, 2010:29). The UK government has allocated £500 million to mitigating the cybercrime threat (Scott, 2010). Clearly, cybercrime losses are significant, not only in monetary terms, but also in terms of national security.

A good source to consult when trying to understand the extent of cybercrime is cybercrime surveys. However, as will be shown later in this section, cybercrime surveys do not provide direct links with hacking activities. Nonetheless, it is possible to infer the link by looking at crimes typically associated with hackers. Before considering some surveys, general crimes committed by hackers from a cybercrime perspective will be discussed.

### 3.10.1 Cybercrimes committed by hackers

Firstly, the most common threat posed by hackers, and one closely linked with the definition of hacking as discussed in section 3.2.4, is unauthorised access to and control over computers. Once access has been obtained, a number of criminal activities, also often classified as cybercrime, might take place. This may include theft of computer resources by storing illegal or illicit material or theft of proprietary or confidential information, including for example software, confidential corporate data, credit card details or personal information. Further examples of crimes committed once access has been obtained include system sabotage, and alteration and destruction of IT systems and networks. This includes hackers altering log files in an attempt to cover their own tracks for fear of being discovered. Website defacement and ‘spoofing’, which could lead to reputational damage for the affected organisation, are other examples of cybercrime which may take place (Yar, 2006:27-28). Cybercrime can therefore be committed together with hacking activities.
Secondly, it is also important in this section to look at crimes committed by hackers. Two activities typically associated with hackers, already highlighted in section 3.2.3 as part of the evolution of hackers, are DoS attacks and distribution of malware or Trojan software (Yar, 2006:30). Writers such as Best (2006:224) have also highlighted DoS attacks committed by hackers. O’Neil (2006:225) and McHugh and Deek (2005:95) have highlighted the destructive and criminal nature of malware deployed by hackers. Thomas (2005:602, 614, 616) points out several crimes associated with hackers, such as DoS attacks, spam, identity theft, worms, viruses and Internet fraud. One particular example is provided by Geissler (2004:163), who explains that a hacker could hack into a user’s mailbox in order to obtain the user’s address book. This in turn can be used to distribute spam messages. Hackers could therefore commit cybercrime activities.

Furthermore, Mukhopadhyay, Saha, Chakrabarti, Mahanti and Podder (2005:153-154) list several reported hacking incidents at financial institutions, which include crimes such as data theft, extortion, credit card theft, compromise of systems and networks, identity theft, disclosure of corporate trade secrets and DoS. Kshetri (2005) points out that some hackers engage in extortion once they have hacked into a victim’s computer system. From a different perspective, the intrusive, damaging nature of cyber-terrorism (as discussed in section 3.5.3.5) committed by hackers is highlighted by writers such as Kracher and Martin (2009:67).

Some of the crimes committed by hackers highlighted in the discussion up to this point are summarised in Table 3.2 below:

<table>
<thead>
<tr>
<th>Table 3.2 Crimes specifically committed by hackers</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Theft of computer resources.</td>
</tr>
<tr>
<td>• Theft of data.</td>
</tr>
<tr>
<td>• Theft of credit cards.</td>
</tr>
<tr>
<td>• Identity theft.</td>
</tr>
<tr>
<td>• System sabotage.</td>
</tr>
<tr>
<td>• Web defacement.</td>
</tr>
<tr>
<td>• DoS attacks.</td>
</tr>
<tr>
<td>• Malware.</td>
</tr>
<tr>
<td>• Spam.</td>
</tr>
<tr>
<td>• Internet fraud.</td>
</tr>
<tr>
<td>• Extortion.</td>
</tr>
<tr>
<td>• Cyber-terrorism.</td>
</tr>
<tr>
<td>• Compromising systems and networks.</td>
</tr>
<tr>
<td>• Theft or disclosure of corporate trade secrets.</td>
</tr>
</tbody>
</table>

The types of crimes associated with cybercrime vary greatly. In section 3.9 various hacking techniques were listed. As discussed, there are many similarities between cybercrime types and hacking techniques. Hacking in principle is a type of cybercrime. This is evident in the results of security surveys, discussed next.
3.10.2 Cybercrime security surveys

Surveys with a predominant focus on cybercrime, provide a view of the significance and extent of cybercrime activity and the financial consequences for organisations. A number of recent easily accessible cybercrime security surveys have been selected for discussion. These can be used by organisations in the financial services industry as a broad benchmark of the prevalence of cybercrime, irrespective of size, location or turnover. Although the focus of these surveys is cybercrime, hackers wittingly are role-players in cybercrime.

3.10.2.1 CSI Computer Crime and Security Survey

The 2010/2011 CSI Computer Crime and Security Survey is the fifteenth of its kind, produced by the CSI, and provides a clear picture of the trends in the types of attacks experienced over the past number of years (Richardson, 2011:1). The 2010/2011 CSI Computer Crime and Security Survey Report reflected the views of 351 respondents who are actively interested in security (Richardson, 2011:3). Of the respondents, 49.8% reported that they did not have to deal with security incidents over the year ending June 2010, 41.1% reported that they had to deal with such incidents and the remaining respondents did not know whether an incident had occurred in their organisation (Richardson, 2011:11).

Importantly, the report reflects on trends in the type of attacks experienced for the 2005 to 2010 reporting period for respondents to this survey, which is presented in Table 3.3.

Table 3.3 Types of attacks experienced by percentage of respondents (adapted from Richardson, 2011:17)

<table>
<thead>
<tr>
<th>Type of attack</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
<th>2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware infection</td>
<td>74%</td>
<td>65%</td>
<td>52%</td>
<td>50%</td>
<td>64%</td>
<td>67%</td>
</tr>
<tr>
<td>Bots / zombies within the organization</td>
<td>Added in 2007</td>
<td>21%</td>
<td>20%</td>
<td>23%</td>
<td>29%</td>
<td></td>
</tr>
<tr>
<td>Being fraudulently represented as sender of phishing messages</td>
<td>Added in 2007</td>
<td>26%</td>
<td>31%</td>
<td>34%</td>
<td>39%</td>
<td></td>
</tr>
<tr>
<td>Password sniffing</td>
<td>Added in 2007</td>
<td>10%</td>
<td>9%</td>
<td>17%</td>
<td>12%</td>
<td></td>
</tr>
<tr>
<td>Financial fraud</td>
<td>7%</td>
<td>9%</td>
<td>12%</td>
<td>12%</td>
<td>20%</td>
<td>9%</td>
</tr>
<tr>
<td>Denial of service</td>
<td>32%</td>
<td>25%</td>
<td>25%</td>
<td>21%</td>
<td>29%</td>
<td>17%</td>
</tr>
<tr>
<td>Extortion or blackmail associated with threat of attack or release of stolen data</td>
<td>Option added in 2009</td>
<td>3%</td>
<td>1%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web site defacement</td>
<td>5%</td>
<td>6%</td>
<td>10%</td>
<td>6%</td>
<td>14%</td>
<td>7%</td>
</tr>
<tr>
<td>Other exploit of public-facing Web site</td>
<td>Option altered in 2009</td>
<td>6%</td>
<td>7%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploit of wireless network</td>
<td>16%</td>
<td>14%</td>
<td>17%</td>
<td>14%</td>
<td>8%</td>
<td>7%</td>
</tr>
<tr>
<td>Exploit of DNS server</td>
<td>Added in 2007</td>
<td>6%</td>
<td>8%</td>
<td>7%</td>
<td>2%</td>
<td></td>
</tr>
<tr>
<td>Exploit of client Web browser</td>
<td>Option added in 2009</td>
<td>11%</td>
<td>10%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploit of user's social network profile</td>
<td>Option added in 2009</td>
<td>7%</td>
<td>5%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Instant messaging abuse</td>
<td>Added in 2007</td>
<td>25%</td>
<td>21%</td>
<td>8%</td>
<td>5%</td>
<td></td>
</tr>
<tr>
<td>Insider abuse of Internet access or e-mail (i.e.</td>
<td>48%</td>
<td>42%</td>
<td>59%</td>
<td>44%</td>
<td>30%</td>
<td>25%</td>
</tr>
</tbody>
</table>
### Table 3.4 Types of security technologies used by percentage of respondents (adapted from Richardson, 2011:33)

<table>
<thead>
<tr>
<th>Type of Technology</th>
<th>2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-virus software</td>
<td>97.0%</td>
</tr>
<tr>
<td>Firewall</td>
<td>94.9%</td>
</tr>
<tr>
<td>Anti-spyware software</td>
<td>84.6%</td>
</tr>
<tr>
<td>Virtual Private Network (VPN)</td>
<td>79.1%</td>
</tr>
<tr>
<td>Vulnerability / Patch Management</td>
<td>67.5%</td>
</tr>
<tr>
<td>Encryption of data in transit</td>
<td>66.2%</td>
</tr>
<tr>
<td>Intrusion detection system</td>
<td>62.4%</td>
</tr>
<tr>
<td>Encryption of data at rest (in storage)</td>
<td>59.8%</td>
</tr>
<tr>
<td>Web / URL filtering</td>
<td>59.4%</td>
</tr>
<tr>
<td>Application firewall</td>
<td>58.5%</td>
</tr>
<tr>
<td>Intrusion prevention system</td>
<td>50.4%</td>
</tr>
</tbody>
</table>

The table above highlight the reliance of participating organisations on traditional security technologies.

#### 3.10.2.2 E-Crime and CyberSecurity Watch Surveys

A survey titled “2007 E-Crime Watch Survey”, conducted collaboratively by CERT, the USSS and Microsoft, had 671 respondents (consisting of CSO magazine readers and members of the USSS Electronic Crime Task Forces), for the period July 2007 to August 2007. Respondents reported that 34% of attacks took place from inside an organisation, 37% from...
the outside and 29% from unknown sources. Although hackers were not specifically identified as a threat agent, it can be reasonably assumed that the incident type often strongly relates to hacking and crime types such as those identified in Table 3.2. Consequently, hackers could have been the possible perpetrators. The survey highlighted the following types of crime incidents, listed in Table 3.5 (CSO Online, 2006:1, 14):

Table 3.5 Crime types as per the CERT 2007 E-Crime Watch Survey, including percentage affected (CSO Online, 2006:1, 14)

<table>
<thead>
<tr>
<th>Crime Type</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus, worms or other malicious code</td>
<td>74%</td>
</tr>
<tr>
<td>Unauthorised access to/usage of information, systems or networks</td>
<td>55%</td>
</tr>
<tr>
<td>Illegal generation of spam e-mail</td>
<td>53%</td>
</tr>
<tr>
<td>Sabotage: information, systems or networks</td>
<td>30%</td>
</tr>
<tr>
<td>Zombie machines and BotNets</td>
<td>30%</td>
</tr>
<tr>
<td>Intentional exposure of private or sensitive information</td>
<td>35%</td>
</tr>
<tr>
<td>Theft of intellectual property</td>
<td>40%</td>
</tr>
<tr>
<td>Fraud</td>
<td>46%</td>
</tr>
<tr>
<td>Phishing</td>
<td>46%</td>
</tr>
<tr>
<td>Theft of proprietary info</td>
<td>40%</td>
</tr>
<tr>
<td>Spyware</td>
<td>52%</td>
</tr>
<tr>
<td>DoS attacks</td>
<td>49%</td>
</tr>
<tr>
<td>Website defacement</td>
<td>24%</td>
</tr>
<tr>
<td>Extortion</td>
<td>16%</td>
</tr>
<tr>
<td>Identity theft of customer</td>
<td>33%</td>
</tr>
</tbody>
</table>

CSO magazine, the USSS, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte collaboratively conducted the “2010 CyberSecurity Watch Survey” for a period of 12 months (July 2008 to August 2009). A total of 523 surveys were completed by participants from various industries in the USA (CSO magazine, USSS, Software Engineering Institute CERT Program at Carnegie Mellon University & Deloitte, 2010:1). Cyber security events affected 60% of respondents, while 37% indicated that they experienced an increase in these events (CSO Magazine, et al. 2010:7). Respondents were of the opinion that 50% of the attacks were perpetrated by outsiders, and 26% indicated that events were perpetrated by insiders. Of the events experienced, 28% were indicated as targeted attacks. The following are the extent of cybercrime types indicated by respondents: viruses, worms and other malicious code (53%); spyware (not including adware or unsolicited advertising, 41%); phishing (38%); unauthorised access to systems or networks (35%); website defacement (14%); and sabotage of systems and data (19%) (CSO Magazine, et al. 2010:9).

When the 2007 survey results are compared with the 2010 survey results, there is actually a small decrease across all cybercrime categories. It is not exactly clear why there should be a decrease. One possible answer could be the notably bigger spending on IT security technologies by participants in the 2010 survey (CSO Magazine, et al. 2009:5). The aforementioned surveys results indicate that there has been an increase in external attacks (37% in 2007 and 50% in 2010).
3.10.2.3 Internet Crime Complaint Centre Surveys

A survey was conducted by the Internet Crime Complaint Centre (hereafter iC³), which is a partnership between the FBI and the National White Collar Crime Center, located in the USA. Internet-related crimes are reported through iC³’s complaints centre logged by complainants from countries across the world, such as the USA, Canada, the UK, Australia and India. The total dollar amount of losses due to Internet-related crimes amounted to $264.59 million for 2008. A total of 275,284 complaints were logged, with the complaint categories including, for example, auction fraud, debit/credit card fraud, Nigerian letter fraud, identity theft, etc. The country with the highest number of perpetrators is the USA, with South Africa being reported as having the seventh highest number of perpetrators (iC³, 2009:2, 3, 4, 7, 9). Hackers, as one of the agents of cybercrime, may also have engaged in the Internet fraud and theft as highlighted by iC³. What this report highlights is the criminal impact of the Internet on everyday life and how Internet-related crimes are growing as a significant threat globally.

The 2009 iC³ survey indicated a 22.3% increase in the number of complaints submitted (336,655), with the total dollar amount of losses due to Internet-related crimes amounting to $559.7 million in 2009 (iC³, 2010:2). South Africa also moved up one ranking (sixth position) as having the highest number of Internet crime perpetrators (iC³, 2010:8).

A comparison of the 2008 iC³ survey results with the 2009 survey results shows clearly there has been an increase in Internet crime. The total dollar amount of losses almost doubled, which highlights the financial impact on the victims. South Africa is also taking up a worryingly prominent position among Internet crime offenders across the world.

3.10.2.4 Seventh annual e-Crime Congress and KPMG e-Crime survey

An e-crime survey, conducted in collaboration between the 7th Annual e-Crime Congress and KPMG, was conducted during February and the first half of March 2009. A total of 307 participants completed the survey, mostly from Europe (78%). In terms of the type of organisation participants, 80% were business-oriented, while there were a smaller number of respondents from government and other organisations. Most organisations (47%) indicated a turnover of more than $100 million (AKJ Associates Ltd. & KPMG International, 2009:3). Theft of customer or employee data by insiders or previous employees was indicated by 64% of respondents as a significant issue (AKJ Associates Ltd. & KPMG International, 2009:8). Concerning the sophistication of attacks on customers, 49% indicated an increase
in sophistication of attacks (AKJ Associates Ltd. & KPMG International, 2009:10). The survey indicated that an increase in malware sophistication has been reported by respondents, with automated attacks being a concern (AKJ Associates Ltd. & KPMG International, 2009:11, 12). The trends in the volume of phishing attacks targeting customers have increased (47%), accompanied by an alarming increase in customer-specific targeted attacks (71%) (AKJ Associates Ltd. & KPMG International, 2009:15). In relation to security solutions which make use of signature detection, 79% of respondents indicated that they did not believe that this particular type of security solution is effective in preventing malware attacks (AKJ Associates Ltd. & KPMG International, 2009:16). Respondents have indicated that a customer's online security may be compromised by infected websites (63%) or infected email (48%) (AKJ Associates Ltd. & KPMG International, 2009:17). Survey respondents have indicated that they are most concerned about external attacks aimed at compromising the network security and stealing business-sensitive data (73%) (AKJ Associates Ltd. & KPMG International, 2009:21). Applications hosted on the web (48%) and mobile data devices (43%) have been highlighted as the attack vectors with the biggest associated risk of being compromised (AKJ Associates Ltd. & KPMG International, 2009:22). In answer to the question whether organisations spend enough time and resources on identifying vulnerabilities that could lead to cybercrime, 62% answered in the negative (AKJ Associates Ltd. & KPMG International, 2009:29). With reference to Table 3.2 and the cybercrime types associated with hackers, only theft of computer resources, spam and extortion were not covered in this survey (AKJ Associates Ltd. & KPMG International, 2009:8, 10, 11, 13, 16, 17, 26).

### 3.10.2.5 UK Cybercrime Report 2009

Garlik, an online identity security expert consultancy firm, published the third consecutive UK Cybercrime Report in 2009. Survey data available in the public domain was used to compile this report. According to its report, UK online banking fraud has increased notably (by 132% from the previous year), mostly due to phishing websites (43,991 reported) which targeted UK banking and building societies. Losses due to online banking fraud in 2007 amounted to £22.6 million and increased to £52.5 million in 2008 (Fafinski & Minassian, 2009:3). Approximately 860,000 (just under 50%) of UK businesses experienced a security incident, and serious breaches were reported by 430,000 UK businesses (24%). A total of 137,600 (16%) unauthorised outsider attacks (which include hacking attempts) have been reported in the survey (Fafinski & Minassian, 2009:14-15).
3.10.2.6 South African cybercrime survey

Cybercrime surveys similar to those discussed in the preceding sections are not conducted in South Africa. A small computer crime survey, which is regarded as the first survey of its kind in South Africa, was conducted as the research component for an Information Security for South Africa (hereafter ISSA) conference paper (Stander, Dunnet & Rizzo, 2009:217). The survey was conducted via an online web-based questionnaire during the third quarter of 2008 (Stander, et al. 2009:220). A total of 60 responses were received, with participants being from mostly small to medium-sized organisations. Respondents were from a variety of sectors, with the IT sector delivering most (33%) responses, followed by the financial sector (18%) and government (15%). At least 20% of the respondents were senior executives and 13% were information security officers (Stander, et al. 2009:220). With reference to computer crime, 45% of South African organisations participating indicated that they had experienced attacks. Most respondents indicated that they experienced 1 to 5 attacks in the last 12 months, with more attacks being committed from the inside. The types of attacks reported are similar to other cybercrime surveys (Stander, et al. 2009:223). Regarding the possible motives behind the attacks, “foreign government political advantage” (28%) and financial reward (25%) ranked the highest (Stander, et al. 2009:223). The total estimated loss due to computer crime, was reported as R57.8 million. Most organisations chose not to report the incidents to the authorities, since respondents believed that law enforcement agencies do not have the skills to investigate the crimes committed (27%) (Stander, et al. 2009:224). Where respondents reported the attacks, 25% indicated that the lack of evidence led to the inability to lay charges against perpetrators (Stander, et al. 2009:225). In answer to the question as to the type of security technologies used in South African organisations, 98% indicated the use of anti-virus software, 97% logical access controls and 93% firewalls. In answer to the question related to security audits, 53% indicated that their own staff members conduct reviews of the “effectiveness of information security” (Stander, et al. 2009:221). The survey indicated that 33% of organisations insource security audits by external companies and 27% performed penetration testing by internal staff (Stander, et al. 2009:222).

3.10.2.7 Cybercrime surveys conclusion

Overall, the surveys indicated a growth in cybercrime activity. All the surveys tend to cover similar cybercrime activities (such as viruses, website defacements and unauthorised access), which indicates the universal nature of this crime. Some surveys expanded their cybercrime types from year-to-year, indicating the growing sophistication of cybercrime. The surveys also showed a greater awareness of cybercrime activity among respondents. More
importantly, the surveys highlighted cybercrime types associated with hackers (highlighted in Table 3.2), emphasising the close relationship. Unfortunately, only one cybercrime survey has been conducted in South Africa. It does however indicate that, similar to other countries, South Africa is also being targeted by cyber criminals.

The surveys further highlighted that monetary losses due to security breaches are increasingly significantly. Although the monetary losses by participants from other countries are generally significantly higher, the monetary losses suffered by South African participants cannot be ignored.

Three of the surveys indicated that attacks could take place either on the inside or outside the organisation. At least one survey indicated that more attacks take place from outside, as opposed to inside the organisation. In contrast, two surveys indicated that insider attacks are more prevalent. In particular, in South Africa the insider risk seem to be more significant, which correlates with some of the media reports on hacking (discussed in section 3.12.3). Some cybercrime types could be dual-purpose, in that both cyber criminals and hackers alike could perform a particular cybercrime. One of the primary objectives of hackers is still to gain unauthorised access to an organisation’s network and systems.

3.10.3 Understanding the relationship between hackers and cyber criminals

Overall, hackers are significant role-players in cybercrime, as is evident from the cybercrime types and the association with hacking activities, as discussed in the preceding section. Hackers are increasingly becoming involved in organised crime, seeking sizeable financial award (Holman, 2010:94). In turn, cyber criminals are using the tactics and techniques of hackers to commit cybercrime (McAfee, Inc. 2009:5). The investment for cyber criminals in professional hacker software is low, while the profits generated from stealing credit cards, retail vouchers and renting out botnets, which generate spam, could be very high. The lack of global legal frameworks complicates the prosecution of cyber criminals, making this a very lucrative avenue for crime (Zwaniecki, 2009). Cyber criminals would also hire hackers on the Internet underground (Constandes, 2008), consequently increasing their success in cybercrime activities. Crime syndicates are emerging, similar in nature to Mafia-operated crime rings, where a “ring leader” recruits a number of hackers to engage in illegal activity. Not merely any hacker is included in these crime rings. Hackers have to prove themselves by building a reputation, before being approached by a crime syndicate. These syndicates are reported to be well organised, including a whole organisation of hackers, “data sellers”, leaders and programmers, each with a defined role and set targets. An example of the type
of cybercrime frequently committed through these syndicates is credit card theft, where the hacker steals the data and the “data sellers” sell it to criminals who use the credit card numbers for fraudulent activities (Cassavoy, 2005; Kirk, 2008). Cybercrime attacks will continue to grow in sophistication with an increased focus on corporate data (Chai, 2009). Clearly, cybercrime will continue to grow and find new avenues of generating illegitimate gains.

<table>
<thead>
<tr>
<th>Thematological research questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Based on the literature review above, the following thematological research questions can be defined:</td>
</tr>
<tr>
<td><strong>Hacker threat</strong></td>
</tr>
<tr>
<td>- The extent to which there is an appreciation, particularly in the banking sector, that there is a direct relationship between cybercrime and hacking.</td>
</tr>
<tr>
<td>- The extent to which there is an appreciation, particularly in the banking sector, that hackers may commit cybercrime.</td>
</tr>
<tr>
<td>- The level or realisation in the banking sector that cyber criminals are using the tools and techniques of hackers to commit cybercrime.</td>
</tr>
</tbody>
</table>

3.11 THE QUESTION OF WHETHER HACKING IS A RISK OR AN EVENT

3.11.1 Introduction

The discussion in this chapter has provided a range of perspectives on the meaning and nature of hacking and of the complexity of the threat that hacking poses. However, in the context of the need for good corporate governance, which is central to this thesis, further analysis of hacking as a threat is required so as to allow for a comprehensive discussion of the available and appropriate responses to the threat in the chapters that follow.

3.11.2 The event component of the term “hacking”

A good starting point to this deeper analysis of the meaning and nature of hacking is to consider the definition of hacking as set out in section 3.2.4, in which it was stated that hacking is associated with breaking into a system. This definition of hacking is supported by similar definitions presented by a number of authors, for example:

- “Hack: to gain access to a computer illegally.” (Merriam-Webster Incorporated, 2008)
- “To get into someone else’s computer system without permission in order to find out information or do something illegal.” (Cambridge University Press, 2008)
“Hacking is illegally breaking into a system over a network connection.” (EC-Council, 2008c:Glossary.13)

“Hacking into a system involves a form of so-called social engineering applied to electronic individuals.” (Chirillo, 2001:45)

“Hacking incidents” are defined by Quigley (2005:242) as follows: “Another significant external threat is the penetration of organisational computer systems by hackers. Such attacks, often termed ‘intrusions’, can be particularly dangerous, as once the hacker has successfully bypassed the network security, he or she is free to damage, manipulate or simply steal data at will.”

The common theme highlighted in all of these definitions is that hacking implies that an act, the act of breaking into a system, is present. To perform this act, a certain skills set is required and a certain outcome is expected, such as disruption of systems. Other expected outcomes include data theft or damage to the system and misuse of the organisation's systems, such as for committing fraud. Further outcomes of hacking will be reflected on in section 3.13. Importantly, it follows that the act of hacking means that an event has occurred for which an appropriate response or responses are required. As an event, hacking takes place at a specific point in time. This is further supported by the fact that the word “hacking” is a verb that is linked to the active component of the term. In support of the view that hacking refers to an event, further reference may also be made to the definition of an event as expressed by Khare (2006:294): “An event is an observable occurrence in a system or network.”

The literature on hacking and security engineering often uses the word “attack” to describe the actions of hackers, for example, network attacks, password attacks and DoS attacks (Anderson, 2001:45, 367; Harris, et al. 2005:14; Skoudis & Liston, 2006:671). This further alludes to the active or event component of hacking. Given that hacking is also classified as a type of cybercrime, as discussed in section 3.10, it is worth noting that Gordon and Ford refer to the following characteristic of cybercrime that speaks directly to the event component of hacking (Gordon & Ford, 2006:14): “It is generally a singular, or discrete, event from the perspective of the victim.”

From the discussion above, it can be concluded that since the word “hacking” is strongly linked to the actions or attack types launched by hackers, the phenomenon of hacking itself can be classified as an event.
3.11.3 The risk component of the term “hacking”

Notwithstanding the argument presented above, hacking is also often referred to as a risk, as has already been documented, through the more colloquial definitions or descriptions of hacking presented above. In itself, the concept of risk is not easily defined, as stated by Valsamakis, Vivian and du Toit (1999:33):

One of the problems of defining risk in a universally accepted manner is that the contexts within which risk can be viewed are so diverse. This gives rise to interpretations and definitions suited only to specific areas of study or disciplines.

Therefore, rather than trying to provide a finite definition of risk in this chapter, a discussion of elements of risk will be explored to clarify whether hacking may also be classified as a risk.

3.11.3.1 Exploring the different elements of risk

Firstly, some definitions of risk include an element of “uncertainty”, linked to a future outcome:

- “Risk is defined as the variation of the actual outcome from the expected outcome. Risk therefore implies the presence of uncertainty” (Valsamakis, et al. 1999:33).
- “A risk is the possibility of suffering harm or loss … A risk is composed of an event, a consequence, and uncertainty” (Caralli, Stevens, Young & Wilson, 2007:53).
- “Risk is the uncertainty of future outcome(s)” (Olsson, 2002:5).

When applying this to the concept of hacking, one could argue that there is an element of uncertainty associated with hacking, since it is not possible to determine the exact likelihood of hacking taking place. Often, hacker attacks go unnoticed, due to the covert nature of hacking (Harris, et al. 2005:14). The future outcome of hacking would be unclear, since it cannot be determined whether the hacker will be successful or not. From this perspective, hacking may be classified as a risk. According to Olsson, the element of uncertainty outlined in his definition of risk also contains an attribute “event” or “action” (Olsson, 2002:6). Olsson therefore also recognises the “event” element of his definition of risk.

Secondly, and most decisively for this discussion, is the “event” component of risk. Some definitions of risk contain the key word “event”, for example:

- “Risks are uncertain future events that could influence the achievement of a company’s

- “Risk is a multi-faceted idea. Risk is about future events, occurrences, or outcomes” (Fishkin, 2006:4).
- “The potential for unwanted negative consequences of an event or activity” (Rowe, as quoted by Merna & Al-Thani, 2005:10).
- “Estimation of risk is usually based on the expected result of the conditional probability of the event occurring, times the consequences of the event given that it has occurred” (Gratt, as quoted by Merna & Al-Thani, 2005:10).

There are three key words in the abovementioned definitions:

- **Uncertain**: The likelihood that an event will take place is unknown.
- **Future**: Undoubtedly, risk is about identifying future events.
- **Events**: As per the definitions of events, it is something specific which can take place at a point in time.

Therefore, risk is linked to an “event” that may or may not take place in the “future”. When applying this to the concept hacking, hacking can be viewed as the event, which may or may not (uncertain) take place in the future. Accordingly, the uncertain future event of hacking can be categorised as a risk. It is not the concept “hacking”, which is the identifiable risk. It is the “event” or actions of hacking, which are the identifiable risks. Or put differently, a risk such as unauthorised access to systems could lead to the uncertain future event of hacking.

In the next section, other definitions of risk will be tested against this view.

### 3.11.3.2 Considering risk equations

The definition of risk can be presented in an equation, as a means of identifying and comprehending the different components of risk. The first equation is probability factored by the impact of the risk, as presented in the following definitions:

- “A risk is a potential problem, with causes and effect; to some authors, it is the harm that can result if a threat is actualised; to others, it is a measure of the extent of that harm, such as the product of the likelihood and the extent of the consequences” (Neumann, 1995:2).
- ISO 27002 presents the following definition of risk: “Combination of the probability of an event and its consequences” (ISO/IEC, 2005:2). A similar definition is used in King III (IoD, 2009b:123).

When compared to the “event of hacking”, one could argue that there is a probability or
likelihood that the event hacking will take place. For organisations connected to the Internet, this probability would be higher compared to smaller organisations who have no online presence. The event of hacking also has some sort of outcome or impact on the target. From this perspective, the event of hacking, or more precisely, the event that leads to hacking, can be classified as a risk.

The second equation found in the literature is the risk equation presented by Landoll (2006:354): “Risk” equals the assets factored by “threats”, factored by “vulnerabilities”. Alberts and Dorofee (2001:30) and Caralli, et al. (2007:1, 17, 20) wrote technical reports for the Software Engineering Institute, discussing risk as part of the Operational Critical Threat, Assets, and Vulnerability Evaluation (hereafter OCTAVE) methodology, where information security risks are established by considering the interrelationships between assets, threats and vulnerabilities, in order to quantify and prioritise information security risks and the potential outcomes to the organisation when the threats are realised. Their interpretation of each component of the risk equation is used as a basis for the discussion that follows:

- **Risks** – The definition by Caralli, et al. provided earlier is best suited for this discussion, since it contains the important element of an uncertain future event.

- **Assets** – Are defined as things that hold value for an organisation (Bornman, 2004:17). The organisation will use the assets to achieve its set business objectives and to generate income (Caralli, et al. 2007:34). IT assets would be one of the critical assets for an organisation. IT assets are both logical and physical in nature and can be grouped into information (including data), systems, software, hardware and people (Alberts & Dorofee, 2001:120). The Communications Security Establishment (hereafter CSE) of the Government of Canada extends this definition, to include “infrastructure, goodwill, money, income, organizational integrity, customer confidence, services and organizational image” (CSE, 1999:87).

- **Threats** – “A threat is an indication of a potential undesirable event. A threat refers to a situation … in which a person could do something undesirable … or a natural occurrence could cause an undesirable outcome. A threat is created when a threat actor exploits a vulnerability” (Caralli, et al. 2007:48). Threats have defined properties, such as asset, actor, motive, access, outcome (Alberts & Dorofee, 2001:126).

- **Vulnerabilities** – “A weakness in an information system, system security practices and procedures, administrative controls, internal controls, implementation, or physical layout that could be exploited by a threat to gain unauthorized access to information or disrupt processing” (Alberts & Dorofee, 2001:126). Bornman (2004:19) defines it as “…a weakness that can be triggered accidentally or exploited intentionally.”
Whitman and Mattord combine all of these components (Whitman & Mattord, 2008:41):

An “attack” is an act or event that exploits a “vulnerability”. It is accomplished by a “threat agent” – or specific instance of a threat – that damages or steals an organization’s information or physical “asset”. An exploit is a technique or mechanism used to compromise an information asset. A “vulnerability” is an identified weakness of a controlled information asset – the absence of controls, or the controls in place are no longer effective.

Therefore, risk can be presented in the form of an equation, highlighting the various components of risk. Two primary examples have been highlighted in this section, the first focusing on the likelihood and impact of risk, and the second focusing on assets, threats and vulnerabilities.

3.11.4 Conclusion

Therefore, it can be deduced that hacking is an event that results from a risk or risks. It can be further deduced that the “attack” relates to the event hacking, where a particular type of attack will be used, such as password guessing. The risk can only materialise into an event when the vulnerability and threat are in the same vicinity (Van Loggenberg, 2003:11). The “threat agent” is hackers, who could execute the “attack”. The target is the organisation’s “assets”, specifically systems or networks, which contain data or information. An “exploit” is used as part of the attack type to abuse the vulnerability, such as a piece of code to cause a buffer overflow or a non-technical attack, such as obtaining a password through social engineering. The “vulnerability” could be anything from a software vulnerability to a weakness in physical controls. The vulnerabilities that exist are in fact risks that can be found organisation-wide.

In concluding on the risk equation, as previously stated, a future event of hacking can be classified as a “risk”. “Risk” (future event hacking) equals “assets”, such as servers and confidential information, factored by “threats”, or “threat actors”, hackers, factored by exploiting known “vulnerabilities”, which are risks that could range from software vulnerabilities to physical access control vulnerabilities.

As regards the complex nature of hacking, it must now be acknowledged that hacking can be viewed as an event that results from a risk or vulnerability that is exploited, and it can be viewed as simply a risk itself. This interpretation of the meaning and nature of hacking that will be used throughout this thesis is set out in Figure 3.3, and will form the basis of the discussion of the range of responses available to address the threat of hacking.
The meaning and nature of hacking proposed in this thesis is time-bound, either taking place now or in the future. An organisation can be hacked at this very moment (Harding, 2002). This action will simply be classified as an event, attack, or security incident and will be the result of a risk or series of risks being exploited. The organisation will protect itself by implementing detective controls, such as firewalls or IDSs (Anderson, 2001:375, 384). Given that hacking may also take place in the future, it is correct to say that the act or event of hacking would pose a risk to the organisation. From this perspective, the risk of the event hacking taking place in the future would be managed differently. The organisation will make use of very specific preventative controls such as conducting ethical hacking assignments to identify and correct security vulnerabilities to prevent successful hacking attempts, as well as to place the risk of hacking within the scope of other business risks. But if hacking is viewed on this basis, it is necessary to understand how prominent a risk hacking would be in the business context to gain an understanding of the extent to which a range of strategies may need to be employed to address the threat of hacking, be it from a preventative or detective point of view.

Figure 3.3  Hacking as event and risk (own deduction)
Thematological research questions

Based on the literature review above, the following thematological research questions can be defined:

**Business risk**
- The extent to which the banking sector views hacking as the event that results from risks such as unauthorised physical access to premises.

**Hacker threats**
- The extent to which the banking sector agrees that hacking may be regarded as an event as well as a risk.
- The extent to which the banking sector views hacking as an uncertain future event.
- The extent to which the banking sector regards hacking as an event that will occur as a result of the exploitation of a range of vulnerabilities.
- The extent to which the banking sector agrees with the distinction of hacking as an event or as a risk.

**Hacking response**
- The extent to which the banking sector agrees that the threat of hacking should be responded to from the perspective of preventative as well as detective points of view.

3.12 THE SIGNIFICANCE OF HACKING IN THE BUSINESS CONTEXT

3.12.1 Introduction

The extent to which hacking is a significant threat in a business context must be considered in some detail. After all, if it is not a significant threat, then very basic preventative and detective controls will be an appropriate approach to the threat. On the other hand, if hacking is a significant threat, even if it is only so in specific industries or organisations with specific characteristics, then a much broader, but also more elaborate, approach is required to deal with the threat. The threat will have to be addressed on a preventative and detective level, mitigating the event of hacking with the former and the risk of hacking with the latter.

3.12.2 Media coverage of hacking incidents in general

The prevalence and diversity of hacking incidents are easily followed in the daily media. Numerous examples of hacker attacks are published regularly in the media across the globe, a few of which will be presented to illustrate the diversity and significance of hacking incidents. It is clear that three broad categories of hacker attacks are prevalent in the media: hacktivism, criminal hacking (mostly in the form of theft of credit card details or email addresses for profit) and finally cyberterrorism (Kingsley, 2011:20). It is also apparent that no organisation is immune from these attacks.
3.12.2.1 Media coverage of hacktivism

Hacktivists were responsible for 58% of reported data theft during 2011 (mostly in the USA), according to Verizon’s annual Data Breach Investigation Report. DoS attacks have been used in many cases to create a diversion, while data was being stolen from the target. More than a 100 million records were stolen during 2011 (Goldman, 2012). Examples of major hacktivism incidents are provided below:

Media reports were dominated by the attacks from the hacktivist groups Anonymous and LulzSec during 2010 and 2011. In an act of hacktivism, the hacktivist group Anonymous attacked MasterCard and PayPal, who suspended their services with the website Wikileaks, which is infamous for releasing sensitive and confidential government documents and communication. MasterCard services were interrupted for an undisclosed period. PayPal services were interrupted for eight hours (Vijayan, 2010). These attacks were in retaliation for the arrest of the creator of the Wikileaks website, Julian Assagne (CBS Interactive, Inc. 2010). This is an example of large-scale hacktivism. The Anonymous hacker group has also been responsible for disclosing confidential emails stolen from a “cyber-security firm” HBGary, which was in the process of investigating hacker breaches at organisations such as DuPont, General Electric, Johnson & Johnson, Walt Disney and Sony. These companies have not disclosed the hacker attacks (Riley & Forden, 2011:18; Ogg, 2011). Anonymous has targeted organisations opposed to music and video piracy, such as the Recording Industry Association of America and the Motion Pictures Association of America. It has also targeted organisations such as the Bank of America and Sony, as well as the government websites of Zimbabwe, in retaliation for the alleged involvement of Mrs Grace Mugabe (the wife of the Zimbabwean president) in illegal diamond mining (Crawley, 2011). In addition, it successfully hacked into Apple and the Australian election database in the early second half of 2011 (Stevenson, 2011). Anonymous is not limited to one group of hackers. These hackers operate from various countries and might have varied hacktivist objectives and targets (Decenella, 2011). The hacker group Anonymous has teamed up with the hacker group Team Poison, to initiate a hacktivist project labelled “Robin Hood”. The objective of this project is to target banks in particular and redistribute their criminal proceeds to various charities (Neal, 2011; Leyden, 2011a). Sony was attacked again during January 2012 by Anonymous and Team Poison, due to their backing of the Stop Online Piracy Act (hereafter SOPA) in the US (Neal, 2012).

LulzSec and Anonymous have continued their attacks during January 2012 in retaliation to the arrest of owner Kim Schmitz and closure of the file-sharing website MegaUpload, which
hosted unlicensed media and software. Anonymous has also threatened to increase the intensity of their attacks, due to the introduction of the Anti-Counterfeiting Trade Agreement (hereafter ACTA), the SOPA and Protect IP Act (hereafter PIPA) (Chirgwin, 2012; Muncaster, 2012).

The members of the hacker group LulzSec have claimed responsibility for some of the successful attacks against Sony (Reisinger, 2011). Several of its members, including the ringleader Hector Monsegur, were arrested by the FBI and Scotland Yard, due to their alleged involvement in hacker attacks against organisations such as CIA, the US Senate and Sony (Bains & Seamark, 2011; Arthur, 2011a; Arthur, 2011c; CNN Wire Staff, 2011; Gearty, 2012). As regards the motives of this hacker group, a purported leader of the group with the hacker handle “Sabu” said that they “exposed the sad state of security across the media, social, government online environments” (Arthur, 2011b). The US Attorney’s Office issued a statement outlining the names of the five LulzSec hackers and also some of the hacking incidents they were responsible for. The statement alleges that over 1 million victims were affected by their attacks (United States Attorney’s Office, 2012). Only a small handful of black hat hackers can cause significant damage to several organisations and tens of thousands of Internet users.

The hacker group “Inj3ct0r Team” claimed responsibility for an attack against the North Atlantic Treaty Organisation (hereafter NATO). According to media reports, the hacker group used a zero-day exploit to compromise a web server, which resulted in the disclosure of 2646 files (Reed, 2011). The social media service, Twitter suffered a significant attack during June 2012, which caused service downtime for several hours (Buenos Aires Herals, 2012).

### 3.12.2.2 Media coverage of criminal hacking incidents

The following are some examples of high-profile hacking incidents reported in the media.

- The Murdoch phone hacking scandal

The media extensively covered the tabloid *News of the World* phone hacking scandal, which started as early as 2003. The voice messages of a number of celebrities and royal staff in the UK were obtained without their permission. Several high-ranking officials and the owners of the tabloid (Murdoch) were questioned and criticised for their involvement (Robinson, 2010; Van Natta, Becker & Bowley, 2010; Cowel, 2011; Hough, 2011). In another incident linked to Murdoch, the Italian news corporation NDS was accused of hacking the encrypted
satellite TV cards of one of its rivals, Nagra France (Kington, 2011). This illustrates how hacking activity could lead to significant reputational consequences, even when the owners are not directly involved in the illegal activity.

- The use of malware as part of hacker attacks

The use of malware by hackers and cyber criminals also continues to increase. Kaspersky highlighted that increasingly hackers and cyber criminals are using malware to perpetrate crime, such as stealing credit card details. He argues that the cyber criminals are creating increasingly sophisticated attacks. He referred to a particular virus, named the Conficker virus, which has infected 10 million PCs worldwide. A virus of this nature has been used to commit cyber warfare and has been found on PCs used in the military and other government institutions. He also claims that viruses such as the Stuxnet virus has unparalleled sophistication and was most likely developed by a particular government (Bottomley, 2011:5). The Conficker virus was successfully used by a hacker group from the Ukraine, who stole an estimated $72 million from banking clients of several countries (The SSU Press-center, 2011; Kitten, 2011). Related to this kind of attack is a “mass-injection” hacker attack, such as the LizaMoon attack, which injected code into more than a million website pages during the first quarter of 2011 (Rigby, 2011).

- Other general hacking incidents

A hacker, Edwin Pena, was arrested in June 2006 in the USA on charges of computer and wire fraud. He stole more than 10 million VoIP minutes, to the value of $1.4 million. This was accomplished by scanning telecommunication organisations’ networks for unsecured ports and reprogramming the networks to accept unauthorised telephone traffic, sold on to prospective buyers. Pena was hiding in Mexico and the US authorities were seeking extradition after he fled to avoid prosecution (Gaudin, 2009). In what was reported as one of the biggest identity theft cases in 2009, Albert Gonzalez, a 28-year-old Miami man, stole a total of 130 million credit and debit card account details from Heartland Payment Systems, based in New Jersey, USA. He faces a 20-year jail sentence if convicted (BusinessDay, 2009). In another incident, regarded as the biggest cybercrime investigation in the USA, the FBI arrested more than 50 hackers, while authorities in Egypt charged 47 alleged hackers linked to a phishing fraud used against American banks (Frieden, 2009). Social media websites, such as Facebook and Twitter are also increasingly under attack. In what is believed to be a phishing scam, a Russian-born hacker with the hacker “handle” (nickname) “kirllos”, obtained 1.5 million Facebook user names and passwords, offering them for sale on
the underground market (Olsen, 2010).

Systems used in operating the Nasdaq stock exchange were hacked during February 2011. Although no sensitive trading systems were compromised, the news of the attacks came as a surprise to the investor community (Bowley, 2011). Access to price-sensitive information could have given hackers a significant advantage (Claasen, 2011:63).

The company RSA Security, known for its SecureID tokens, used to provide an additional layer of security to access a network, was compromised during March 2011. A carefully crafted email with an imbedded exploit was sent to unsuspecting employees. A backdoor was installed by the exploit. Hackers used this access to steal details, which allowed them to compromise the defence contractor Lockheed Martin. This attack was successful due to the combination of social engineering, phishing, software exploit and backdoor software (Goodin, 2011). This was a very embarrassing incident for RSA Security, and demonstrates that even well-known security companies are not immune to hacker attacks.

A significant security breach occurred involving the company Global Payments, which facilitates credit card payments with companies such as Visa and MasterCard. Allegedly, 10 million card numbers have been compromised, and hackers have already started using the card details. Visa confirmed the breach. Security researchers believe that the Payment Card Industry Data Security Standard (hereafter PCI-DSS) is not adequate anymore to protect clients from fraudulent transactions. Stealing credit card details has become an easy target for hackers (Pepitone & Remizowski, 2012).

### 3.12.2.3 Media coverage of cyberterrorism

The media also reports on hacking incidents, which poses a threat to the national security of a country. The use of DoS attacks is frequently cited, such as during the feud between Russia and Georgia, when Russian hackers were believed to have attacked Georgian websites (mostly government and media-related sites), during the same time the military campaign was taking place against Georgia during 2008 (Danchev, 2008). CNN also reported on attacks against the Pentagon, which commenced during 2007, such as the attack during which a hacker stole classified files containing details of the US Air Force’s Joint Strike Fighter aircraft programme (Mount, 2009). In another incident, close to 1300 PCs located in various countries were attacked and found to be part of an espionage network based in China. It is not clear who was behind these attacks; however, it is clear that a significant amount of damage could have been done via the cumulative effect of all the
infected PCs. Mostly government-type institutions were infected during these attacks, which started as early as 2007 (CNN.com, 2009).

North Korean hackers have also been accused of launching attacks against South Korean websites, including military and banking websites, as an act of cyberwarfare (Kim, 2009). Iranian authorities reported that 30 000 PCs had been infected with the Stuxnet worm. Security analysts claim that Stuxnet is the most sophisticated malware discovered to date. The worm focused on infecting SCADA (supervisory control and data acquisition) systems, used to operate power plants and military installations. Researchers claim that Iran’s Bushehr nuclear reactor was targeted (Keizer, 2010; Kingsley, 2011:20).

Google reported a “sophisticated” hacker attack against its system during January 2010, which resulted in the theft of intellectual property. It is believed that the attacks were made by hackers based in China, with possible military affiliation (Lee & Hornby, 2010). The US secretary of state Hilary Clinton expressed her concern regarding hacking attacks against Google, in what seemed to be an effort to obtain password details of US government officials who use Gmail accounts (free email accounts in the Internet). It is alleged that the attacks originated from China, although this is denied by the Chinese government (Dombey, Hille, Waters & Menn, 2011).

During February 2011, a hacker group carrying the name “Iran cyber army” claimed responsibility for attacks against “Voice of America” websites. The group protests against what they regard as false propaganda (CNN.com, 2011). Also during the same period, the Canadian government reported a “concerted and sophisticated cyber attack” aimed at disclosing confidential financial data (Newton, 2011). These are all possible examples of cyberwarfare. Another high-profile attack against the International Monetary Fund (IMF) was reported. It is rumoured that the attack was committed by hackers from a “foreign government” who stole several confidential documents (Paul, 2011).

3.12.3 Media coverage of hacking incidents in South Africa

A combination of insider manipulation of systems at Vodacom and phishing attacks against South African bank clients led to charges of fraud to the value of R7 million (Lieberum, 2009; Nkosi, 2009), as discussed in section 3.5.3.6. There has also been a significant increase in the use of phishing attacks targeting South African online banking users. Losses of between R100 000 and R700 000 from South African banking clients were reported during 2007 (Peters, 2007:13; Rondganger, 2007:1; Gerretszen, 2008; Knowler, 2008; Ryan, 2010a:6).
Although phishing attacks continue, the banking sector’s introduction of anti-phishing software has led to a decrease of phishing attacks during the first quarter of 2011, with the average loss amount decreasing to below R5000 (Miller, 2011:1).

Hosken (2008) reported the arrest of an Internet-based syndicate that stole more that R400 million from South African government departments during 2008. Their modus operandi was to steal government employee login credentials, and then to transfer money, via electronic fund transfers (hereafter EFTs), to fictitious bank accounts. The Department of Housing, Local Government and Traditional Affairs lost R199 million during the period 2006 to 2008, through a similar type of cybercrime (Botha, 2008:1). In a similar example, the education department in Mpumalanga lost R5.5 million from its bank account, after hackers allegedly obtained account login details from an insider (Viljoen, 2009). Allistair Peterson spent a year in jail after he stole R55 million from government departments. As part of a plea bargain, he developed award-winning anti-hacker software during 2007 for the defunct Scorpions (an agency that investigated organised crime and corruption), while his eight year sentence was suspended (Chauke, 2009; Electronic Media Network (Pty) Ltd. 2012).

Non-financially motivated hacking incidents also occur, such as the website of the Democratic Alliance (the second-biggest political party in South Africa), which was hacked during August 2008 (Citizen Reporter, 2008:4). The website of the ANC Youth League has been attacked five times by unknown attackers. Security experts pointed out that the security of this website was rather weak, which portrayed the ANC Youth League in a negative light (Bauer, 2011). The attacks discussed above are of a political nature, categorised as hacktivist activity, as explained in section 3.5.3.2. Local ISPs offering website hosting and bandwidth are also frequently targeted by hackers. An example here is MWEB, which claims that it detects approximately 5000 attacks a day, with the occasional attack being successful (Alfreds, 2011).

Maree, a detective from the South African Police Service’s Cyber Crime Support Service, has expressed his concern over the increase in hacking activity and the increased involvement of hackers in organised cybercrime syndicates. The unit investigates hacker threats that range from identity theft, malware attacks, phishing, spam and botnet attacks (Burrows, 2009:18). From a phishing attacks perspective, the RSA Anti-Fraud Command Centre reported that South Africa was the third most attacked country globally in February 2011. It is estimated that South Africa lost R1 billion over the last three years due to cybercrime (Buthelezi, 2011:7). According to Sabric, phishing attacks against South African citizens are a lucrative crime, even though only a few customers out of a million might
actually respond to a phishing attack (Miller, 2011:1).

FirstRand claimed that its 2010 interim financial results might have been disclosed prematurely, with a targeted hacker attack given as the explanation for why the financial results were disclosed. This led to FirstRand bringing forward the official disclosure date of its 2010 interim results, which may have also contributed to the fall in FirstRand’s share price at that time (Crotty, 2011:13).

Although most of the hacker incidents reported in the media were unsophisticated attacks, the incidents nonetheless led to significant financial losses. Hacker attacks are not only crimes committed abroad, but are also a reality within the South African context.

3.12.4 Factors increasing the hacker threat in South Africa

The Internet has undeniably become one of the most critical communication networks of today. It allows organisations and individuals to communicate and transact not only locally, but also abroad. It affects our daily lives, similar to other networks, such as telephone and transportation networks. There is a significant difference, though, from other networks, in that the Internet does not have an overarching body that monitors the use of the Internet, which leaves it open for criminal and inappropriate use (Cordell & Neogi, 2007:1-5).

South Africa’s Internet user base has passed the 5.3 million-user mark and was expected to grow to 6 million by the end of 2010. The user base is expected to grow past the 10 million mark by 2013. Significant regulatory restrictions might be amended, leaving the market open to new role-players and increasingly cheaper bandwidth. This will lead to more and more businesses, in particular smaller business operations, connecting to and conducting business on the Internet (World Wide Worx, 2009:1-3; SouthAfrica.info, 2010). More South Africans are starting to make use of smartphones as a means of staying connected to the office. Since smartphones can be easily lost, the risk of identity theft will continue to grow in South Africa (Dingle, 2009b). South African Internet users are among the fastest growing users of social networking sites, such as Facebook, with more than 3.7 million South African users registered on this online application. Many new viruses are being introduced by social media websites such as Facebook (De Sousa, 2008; Benjamin, 2011:4). South Africans are therefore also spending more time on the Internet, also increasing the likelihood that they will be affected by the hacker threat.

International bandwidth provisioning is also on the increase, linking South Africa to the rest
of the world. This increases cybercrime. Telkom used to be the only provider of international bandwidth. Now, Neotel provides additional international bandwidth to South Africa via the submarine cable system Seacom (Grobler & Jansen van Vuuren, 2010:1-2; Seacom, 2011). Even more bandwidth is provided by EASSy, a competing undersea cable with multiple owners, which also provides additional international bandwidth to South Africa (Dingle, 2009a; EASSy, 2010). South African organisations have to consider the possible influx of bigger and more sophisticated hacker attacks, as a consequence of bigger international bandwidth.

3.12.5 Surveys reflecting on the significance of hacking and cybercrime

In order to further understand the extent of hacking and cybercrime, and the effect it has on business, the results of a number of surveys from a range of organisations will be presented here. These surveys will further highlight concerns around IT risk, IT security, product spending, losses suffered in attacks and the trends in hacking and cybercrime.

3.12.5.1 Surveys by PricewaterhouseCoopers

Three of the big four audit firms (PricewaterhouseCoopers, Deloitte and Ernst & Young) annually publish surveys on information security, based on industry trends across their extensive client base. Since they are leaders in providing information security and IT audit services, their surveys are of particular importance in the context of this thesis. The only exception is KPMG, which has not conducted an information security survey recently (Yahoo!, 2012). The first firm's survey to be presented is that of PricewaterhouseCoopers (hereafter PwC).

PwC conducted a global information security survey during the third quarter of 2009. This survey has been cited by writers such as Townsend (2010:22). The survey was completed by 7200 Chief Executive Officers (hereafter CEOs), Chief Financial Officers (hereafter CFOs), CIOs, Chief Information Security Officers (hereafter CISOs), Chief Security Officers (hereafter CSOs) and other executives responsible for IT and security investment in 130 countries. The economic downturn that began in 2009, had a significant effect on information security spending. The spending on information security has in fact decreased (12% of respondents in 2009, as opposed to 5% for 2008, indicated that spending would decrease). At most, 47% of respondents indicated that their organisations reduced budgets for security initiatives, although the degree of reduction differs. The impact of the economic downturn had varying effects: 56% of respondents indicated that the regulatory environment is
increasingly becoming more complex and burdensome; 52% of respondents indicated that the role and importance of the information security function has increased due to an increased risk environment; and 43% of respondents indicated that threats to information security have increased. In general, organisations reported improvements in information security governance, such as by appointing a CISO (15% more than in 2008) (PwC, 2009a:3, 6, 9, 11, 15).

PwC also compiled a survey with the CIO Magazine and the CSO Magazine collaboratively, titled “Eye of the storm. Key findings from the 2012 Global State of Information Security Survey”, that was conducted online between February and April 2011. The results are based on the responses of more than 9 600 CEOs, CFOs, CISOs, CIOs, CSOs, vice presidents and directors of IT and Information Security representing 138 countries (PwC, 2011:B). More organisations have invested in information security safeguards, such as malicious code detection tools (72% of respondents in 2010, increasing to 83% of respondents in 2011) and intrusion prevention tools (61% of respondents in 2010, increasing to 74% of respondents in 2011) (PwC, 2011:12). Spending remains a priority on information security initiatives, although marginally lower (1% less from 52% of respondents in 2010) when compared to the previous year (PwC, 2011:13). Advanced Persistent Threat attacks (a targeted and sophisticated hacker attack, sometimes funded by foreign governments) have been identified as a significant concern for many organisations. A total of 38% of respondents indicated penetration testing as a response to this threat during 2010 and 2011 (PwC, 2011:15). An interesting trend is that in terms of the effectiveness of information security activities, the overall percentage of those that believe their practices are effective has declined every year since 2006 (84% down to 72% in 2011) (PwC, 2011:18). Mobile devices and social media have been identified as technologies posing a significant risk to organisations. Only 43% of organisations have a security strategy in place to govern the use of personal devices in organisations (PwC, 2011:22).

3.12.5.2 Surveys by Ernst & Young

Already in its 13th year of publication, the trends reported in the latest two annual global information security survey produced by Ernst & Young will be discussed next. The 12th annual global information security survey, focus on how organisations deal with change, risks, new regulatory requirements and new technologies (Ernst & Young, 2009:3). The report is quoted by the Australian Institute of Company Directors (2010:5) and the International Association of Privacy Professionals (2010). A total of 1900 diverse organisations participated in the survey, with participants spread almost equally over the
USA, Asia and Europe (Ernst & Young, 2009:22). Respondents indicated that at least 50% of them started spending more on improving security risk management, while 39% continued to spend equal amounts on improving security risk management (Ernst & Young, 2009:4). Regarding the adequacy of budget for information security spending, 19% indicated that this was a significant challenge (Ernst & Young, 2009:8). From a hacking perspective, 41% indicated an increase in external attacks, including phishing and website attacks (Ernst & Young, 2009:5). The role of information security is regarded as significant in protecting the reputation and brand (61%), ensuring privacy and protection of confidential personal information (53%) and attaining regulatory compliance (46%) (Ernst & Young, 2009:12).

Ernst & Young’s 13th annual global information security survey focuses specifically on emerging technologies. The survey was conducted between June and August 2010. In total, 1600 organisations participated, from countries across the world (EYGM Limited. 2010:18). The survey indicated that 60% of respondents faced increased risk due to technologies such as social networking, cloud computing and mobile computing devices (EYGM Limited. 2010:2). The availability of IT systems has been identified as a top priority for organisations, followed by the risk of sensitive data disclosure (EYGM Limited. 2010:5). Data leakage, loss of visibility of company data and unauthorised access have been identified as the three key risks associated with cloud computing (EYGM Limited. 2010:10). The use of data leakage prevention technology has also been identified as the preferred option for protecting against data leakage (EYGM Limited. 2010:6). Hackers are not mentioned as role-players in this survey.

### 3.12.5.3 Surveys by Deloitte

Deloitte produces information security surveys for various industries, two of which will be discussed next. Deloitte produced a survey, which looked into information security in the financial services industry. More than 350 global financial organisations were interviewed. They ranged in size, with respondents mostly from the banking sector (54%), followed by the insurance sector (21%) (Deloitte Touche Tohmatsu, 2010a:2). Of the respondents, 52% indicated a high threat perception related to the increase in sophistication in threats. Hacker attacks against emerging technologies, endpoint devices and exploitation of insecure code are in sixth, seventh and eighth place respectively (Deloitte Touche Tohmatsu, 2010a:25). Specifically pertaining to hacking as a means of stealing information, 7% of organisations indicated at least one attack and 4% indicated repeated attacks (Deloitte Touche Tohmatsu, 2010a:26).
Another survey conducted by Deloitte, focused on information security challenges in the technology, media and telecommunications industry. Interviews were conducted with 138 large organisations worldwide during 2011 (Deloitte Global Services Limited, 2011:4). The survey indicated 18% of technology organisations indicated that they experienced six to 20 breaches in the past year. Greater awareness by the public increases the sensitivity associated with these breaches (Deloitte Global Services Limited, 2011:6). Regulators have higher expectations from an information security perspective, which leads to increased spending on compliance initiatives (Deloitte Global Services Limited, 2011:8). Results indicated that 60% of respondents recognise the threat posed by third party connections and the need to identify the third-parties information security practices (Deloitte Global Services Limited, 2011:10). In terms of the focus areas for information security executives, data and information privacy (76%) is a top concern, followed by risk management (56%), disaster recovery plan (hereafter DRP) (51%) and physical security (43%) (Deloitte Global Services Limited, 2011:12). More organisations are allowing their employees to use their personal mobile devices for “work-related activities” (Deloitte Global Services Limited, 2011:14), despite mobile devices being regarded as one of the biggest information security threats (Deloitte Global Services Limited, 2011:16).

3.12.5.4 Surveys by BERR, Infosecurity and PWC

A survey titled “2008 Information Security Breaches Survey: Technical Report”, was conducted by the UK Department for Business Enterprise & Regulatory Reform (hereafter BERR). This study has been cited by a number of writers, such as Rhee, Kim and Ryu (2009:817, 824), Talib, Clarke and Furnell (2010:196, 199, 203) and Furnell and Thomson (2009:5, 10). The objective of the survey was to conduct research into information security breaches in the UK, helping businesses in the UK to focus on the risks they face (BERR, 2008:1). A total of 1007 “computer assisted telephone interviews” were conducted. Respondents were from various sectors and various sizes of business. A total of 68% of large businesses who participated in the survey indicated that they experienced malicious security incidents. The survey highlights that this percentage is not an accurate reflection of the total number of security breaches, since many organisations still lack the technology to monitor and identify security incidents. A total of 39% of respondents indicated that large organisations experienced unauthorised outsider attacks, which include hacking attempts. A total of 13% of respondents indicated that they experienced successful hacking incidents. The biggest impact of security breaches is business disruption, with an average cost of £15 000 for two days for small companies and £130 000 for two days for larger companies. The survey also presents examples of actual incidents, which highlights that some organisations
suffered severe business disruption and that their business continuity plans (hereafter BCPs) failed to facilitate the recovery of their organisations adequately. The total cost of incidents was estimated at £170 000 for large businesses and £2 million for very large organisations. Only a few companies reported a loss of reputation due to security breaches, yet this does remain one of management’s biggest fears (BERR, 2008:22, 23, 24, 27, 29, 31).

The second survey considered is that on information security practices and incidents in the UK. The survey was conducted annually since early 1990 by these UK government departments: BERR, the Department of Trade and Industry (hereafter DTI) and the department for Business Innovation and Skills (hereafter BIS). The 2010 survey, compiled by Infosecurity Europe and PwC was directed to 539 organisations featuring a wide range of businesses (Infosecurity Europe & PwC, 2010:1). According to the survey, 92% of large respondents experienced a security incident in the last year (72% in 2008). The cost of the incidents ranged between £280 000 to £690 000, which is a significant increase from the maximum of £170 000 reported in 2008 (Infosecurity Europe & PwC, 2010:2). As regards malware and hacking, 62% of large organisations reported malware attacks; 61% indicated a significant attempt to break into the organisation (48% for smaller organisations); 15% reported actual hacker breaches (11% for smaller organisations); and 25% reported DoS attacks (18% for smaller organisations) (Infosecurity Europe & PwC, 2010:3, 15). With reference to the actual number of attacks, 13% of respondents indicated that they detected hundreds of attacks per day. Up to 5% of respondents reported successful hacker breaches several times a day (Infosecurity Europe & PwC, 2010:15). Regarding security breaches in general, 92% of large organisations and 83% of smaller organisations experienced malicious security incidents (Infosecurity Europe & PwC, 2010:10).

3.12.5.5 Surveys by (ISC)²

Another survey to consider, sponsored by the International Information Systems Security Certification Consortium (hereafter (ISC)²), is the 2008 (ISC)² Global Information Security Workforce Study. This study has been cited by a number of writers, such as Colley (2010:16) and Grossman (2008:24). The intention of the survey is to identify significant trends and opportunities emerging from the information security profession worldwide. There was a total of 7548 respondents, from mostly America, Europe, Middle East and Africa, and Asia-Pacific. Hackers and insider employees (51%) were seen as the second-biggest threat to an organisation, after virus and worm attacks. The damage to an organisation’s reputation was seen as the second-biggest priority organisations were faced with (Frost & Sullivan,
2008:2). The reputation of an organisation is clearly then an aspect that needs to be further explored.

3.12.5.6 **Surveys by Wolfpack Information Risk (Pty) Ltd.**

An independent survey done by the company Wolfpack Information Risk, and endorsed by the Information Security Group of Africa (hereafter ISG) and the South African Chamber of Commerce and Industry (SACCI), provides some insight into the current practices of information security management at selected South African organisations. Participants from 77 South African companies of various sizes, mostly from the financial, telecommunications and government sectors, completed the survey (Wolfpack Information Risk (Pty) Ltd. (hereafter Wolfpack) 2011:6). A large number of participants fulfil the role of ISO or CISO (48%) (Wolfpack, 2011:5). The survey highlights that more than 30% of medium to large organisations still do not have an ISO in place. A total of 48% of organisations do not have an information security charter in place (Wolfpack, 2011:9). A total of 45% do not have an information security steering committee in place (Wolfpack, 2011:9). In terms of applying the principles defined in King III, 56% indicated that their boards of directors had not assumed responsibility for information security governance (Wolfpack, 2011:11; IoD, 2009b:87). Only 18% indicated that they are fully compliant with the requirements of King III (Wolfpack, 2011:18). Only 30% of respondents’ board of directors have included information security as an agenda point (Wolfpack, 2011:12). The survey also highlights that information risk has not been fully incorporated into Enterprise Risk management (hereafter ERM) at 47% of the organisations (Wolfpack, 2011:15). A total of 46% of respondents indicated that their organisation’s major IT risks have not been incorporated into ERM (Wolfpack, 2011:16).

3.12.6 **The effect of hacking on an organisation’s reputation**

From the surveys above, it is evident that actual monetary losses were the outcome of hacking incidents. This is not the only damage an organisation can suffer from such an incident, however. Such incidents can also have a notable effect on the reputation of an organisation (Trend Micro Inc. 2008:8; O’Reilly, 2008:12), a significant business risk which will be discussed in section 4.3.11. Reputational losses are difficult to quantify. The information security survey conducted by PwC during, referred to in section 3.12.5.1, indicated that 32% of respondents saw the organisation’s reputation as a driving factor behind information security spending. The reputation of an organisation therefore becomes an asset, which could also be under threat by hacker attacks (PwC, 2009a:7, 39). Glaessner, Kellermann and McNevin also concur that reputational losses are difficult to
quantify. It is suggested that the fear for reputational consequences may lead to non-disclosure of hacking incidents and other e-crimes to the authorities or even force organisations to pay money to the extortionists. Disclosure of hacking incidents could lead to a lack of public confidence and loss of business (Glaessner, Kellermann and McNevin, 2002:10-11, 16). Clearly then, reputational damage leads indirectly to losses

McAfee conducted a survey on the effect of data losses on organisations. Included in the survey population were a 1000 large organisations and dozens of security and business experts from top institutes. The survey indicated that 50% of respondents were more concerned about the damage the incident would cause to the organisation’s reputation than its economic (33%) or regulatory (16%) impact (McAfee, Inc. 2009:7). Similar concerns were raised by Burdon, Lane and Von Nessen (2010:116) regarding the reputational consequences of notifying authorities of data breaches, as required by US, Australian and European Union legislation. They specifically highlight hacking incidents as one of the causes of personal information data breaches and how that could lead to embarrassment for the organisation affected (Burdon, Lane & Von Nessen, 2010:115, 126). A study conducted by Ponemon in the US during 2008 indicated that the average cost for recovering from a significant data breach per organisation (43 organisations across a number of industries) is $6.6 million. Healthcare and financial services industry reported the highest losses (Ponemon, 2009:4, 6).

A survey conducted by Symantec, covering 200 senior level managers across a wide range of industry sectors, indicated that where participants experienced data losses, 42% claimed that they suffered reputational damage (ITNewsAfrica, 2009b). Both tangible and intangible assets could be severely affected by hacker events.

3.12.7 Conclusion

Hacking incidents are often reported by the media. The same applies to the South African media, with a particular focus on hacking incidents in the banking industry. Numerous factors are leading to the proliferation of hacking incidents in South Africa. These include an increase in the South African Internet user base, with even further growth expected due to a decrease in bandwidth cost.

Information security and cybercrime surveys highlighted the continued growth in cybercrime activities, which include hacking. The incidents and trends highlighted by the surveys indicate that cybercrime and hacking are significant concerns for organisations, leading to
financial losses, increased spending on information security solutions and continued vigilance to respond appropriately to these threats to ensure their business is not adversely affected. It has also been pointed out that the effect of hacking on an organisation’s reputation could lead to regulatory penalties, loss of business and a decrease in the public’s confidence.

**Thematological research questions**

Based on the literature review above, the following thematological research questions can be defined:

**Business risks**
- The extent to which there is an appreciation in the banking sector that hacking incidents are frequently reported in the media and the possible resulting reputational consequences this may have.
- Consideration for all possible outcomes of a hacking attack in the banking sector, such as loss of data or customers, and loss of reputation.
- The extent to which the banking sector will be able to understand the risks and complexities associated with hacking.

**Hacking threats**
- Whether there is an appreciation of the factors which could lead to an increase in hacking incidents in the banking sector.
- The extent to which the banking sector understands the risks and complexities associated with hacking.
- The extent to which the interrelationship between cybercrime and hacking is understood in the banking sector.
- Whether there is an appreciation for the factors which will lead to an increase in hacker activity in South Africa, such as cheaper bandwidth and an increased uptake of cellphone banking.
- Whether the banking sector realise that the threat of hacking is growing and combining with cybercrime to become an even bigger threat.

**Hacking responses**
- The extent to which the banking sector takes notice of information security surveys and the message the surveys are trying to convey.
- The extent to which the banking sector's information security addresses the risks associated with hacking.
- The extent to which the banking sector uses IT risk management to address the threat of hacking.

### 3.13 FINAL OBSERVATIONS ON THE EFFECTS OF HACKING

Now that it has been established that the event of hacking or the risk of hacking is significant in the business context, particularly in the financial services industry, what remains is to provide a synopsis of what the effect of hacking is – or, to put it more bluntly, “what actually happens if we are being hacked”. Even though the intention of this section is not to provide a comprehensive list of the effects of hacking, this will assist in the discussion of the responses available (chapter 5) to deal with hacking and will be incorporated in the fieldwork.
conducted for this thesis.

- The first example of the effects of hacking was discussed in section 3.3.2 with the discussion of the profile of script kiddies. There, the outcome of a DoS attack was highlighted as one of the first effects of hacking. DoS implies that a particular business service or process will either become unavailable or extremely slow as a result of the sheer volume of traffic created, flooding the target system, slowing it down or even disabling it entirely. A DoS attack can cause a lot of disruption and financial damage to organisations (Arbor Networks, 2005:9). Examples of DoS attacks abound and are frequently cited in the media, as highlighted in section 3.12.2.3. As highlighted in section 3.5.3.1, not only actual DoS attacks, but also the mere threat of a possible attack might cause a damaging setback to the organisation.

- As documented in section 3.5.1, hackers may simply break into a system because they have the required skill and for the thrill of it (Beaver, 2004:25). Alternatively, they may break into a system to collect information that they may use in later attacks, as mentioned in section 3.3.3 (Arief & Besnard, 2003:2) or to escalate system privileges (Singleton, 2008:11-12), as discussed in section 3.8. As the hacker can then conduct unauthorised transactions, possibly even without detection. As explained as part of the hacker methodology in section 3.6, hackers may engage in a thorough planning process (Skoudis & Liston, 2006:183), in particular where the security measures implemented are challenging to breach. Even a more cautious approach can be taken, as discussed in section 3.3.7, by breaking into an organisation without causing any damage and simply providing proof that it is possible to break into the organisation (Denning, 2006; Stamatellos, 2007:17).

- Section 3.3.2 and 3.3.3 points to the fact that a malicious hacker attack can cause damage to a system or organisation (Buys & Cronje, 2004:327). The damage could be intentional or accidental. Accidental damage is caused when the attacker unknowingly damages or deletes files, data and software on the compromised system, compromising the integrity of the files and data (Embar-Seddon, 2002:1037). This is in particular the case for inexperienced script kiddies (Best, 2006:215), whose attacks could lead to damage to computer and network equipment worth tens of thousands of Rands, including IT staff and management’s time to recover the affected systems (Nissenbaum, 2004:199). Intentional damage takes place when the hacker has a motive for causing deliberate damage to the compromised system, such as revenge, and changes personal records or erases evidence of misconduct. Divulging to the
public how the attack was conducted could lead to reputational consequences for an organisation (Tiller, 2005:29-31; Skoudis & Liston, 2006:627-628).

- As highlighted in section 3.3.3, crackers could also circumvent copyrighted software, making it freely available to users on the Internet or by simply using it for either commercial or criminal gain (Newman, 2006:75). Über hackers could also make use of their reverse engineering and programming skills to circumvent copyrighted software, as mentioned in section 3.3.4 (Day, 2003:129). This will lead to the illegal use of copyrighted software and direct losses for the developers of the software.

- As pointed out in sections 3.3.3 and 3.4, crackers could make use of system resources, such as creating covert communication channels, to communicate with fellow hackers or by storing files on an organisation’s systems, without having to pay for the storage space (Arief & Besnard, 2003:13; Newman, 2007:1). In doing so, valuable system resources are being used. Once a hacker manages to break into a target, he or she will have to maintain access (as discussed in section 3.6). Hackers even go as far as using the business applications to process transactions, returning to the organisation’s system on a regular basis (Ashley, 2004:43-44; Protalinski, 2008).

- Über hackers propagate the field of hacking (mentioned in section 3.3.4) by developing automated hacker software and “how to” guides, which are subsequently used by less skilled hackers or script kiddies (Beaver, 2004:23; Schell & Martin, 2004:53; Yar, 2006:32). Similarly, as discussed in section 3.3.5, black hat hackers could sell exploits on the underground market (Bloor, 2007; Naraine, 2006). This increases the likelihood of successful hacking attempts and exposes more organisations to the threat of hacking.

- As documented in section 3.3.5, black hat hackers often pursue a profit motive. Their actions may therefore include stealing anything from credit card numbers and trade secrets to confidential client data (Basta & Halton, 2008:3). Hackers may even go as far as trying to sabotage their own hacker competitors for financial reward, as discussed in section 3.5.1 (Schell & Martin, 2004:2). Hackers could offer their services to organised crime syndicates, as discussed in the last section of 3.10. (Skoudis & Liston, 2006:8-9; Beaver, 2004:24; Krone, 2005a). Another approach to profit from hacking is through extortion (Tiller, 2005:31). Insiders might also be motivated by the possible financial gain to be attained by stealing and selling organisational confidential
data, as mentioned in section 3.5.3.6 (Aeran, 2006:15). Increasingly, hackers are driven by the need for financial reward.

- Sections 3.3.7 and 3.5.3.2 highlighted that hacktivist groups could distribute their activist message through website defacement (Pearce, 2002:14; Osborne, 2006:277; Basta & Halton, 2008:3). This will prevent the target organisation’s supporters from reaching the organisation’s website or stop them from publishing their intended message (Zager, 2002; Taylor, 2005:634; Manion & Goodrum, 2007:61; Stamatellos, 2007:16). Web defacements could also lead to loss of clients, public humiliation or reputational losses. Hackers may also engage in acts of terrorism (section 3.5.3.5), which may affect the telecommunications infrastructure and power utilities supporting the organisation (Skoudis & Liston, 2006:8; Beaver, 2004:24; Schell & Martin, 2004:23). Direct attacks are also possible, when for example online banking facilities are targeted, to destabilise the financial backbone of a particular country (Aaviksoo, 2008:29).

- Hacking is closely related to cybercrime, increasing the possible negative consequences for an organisation. This includes industrial espionage (Tiller, 2005:32), covered in sections 3.5.3.4 and 3.5.3.6; theft of hardware, removable storage media or even mobile phones which may contain contact details, or even confidential information (covered in section 3.8.3); making use of malware to advance attacks (mentioned in sections 3.8.3.2 and 3.10.1) and illegally using system resources, and committing theft, industrial espionage and extortion (discussed in section 3.10) and listed in Table 3.2.

- Lastly, as pointed out in section 3.3.3, crackers often engage in social engineering activities to obtain more information on the target organisation (Arief & Besnard, 2003:3). As mentioned in section 3.5.1, hackers may steal identities, consequently masquerading as legitimate users (Schell & Martin, 2004:2). Social engineering, dumpster diving and gaining physical access to an organisation’s premises (discussed in section 3.6) are non-technical techniques of obtaining general organisational information that may be used to plan an attack (Thornburgh, 2004:133; Skoudis & Liston, 2006:184, 193, 195). These almost non-intrusive techniques could lead to significant hacker attacks.
Thematological research questions

Based on the literature review above, the following thematological research questions can be defined:

Business risk
- The extent to which the banking sector can respond to the reputational consequences of web defacements and hacker attacks being made public in the media.
- The extent to which the banking sector realises that hacktivists could negatively affect the image and brand of a bank.

IT risk
- The extent to which the banking sector realises that hacker attacks could lead to damage to systems and data.

Hacker threat
- The extent to which there is an understanding that the mere possibility of DoS attacks could pose a threat to the banking sector.
- The extent to which the banking sector realises that it might be attacked by hackers without their knowledge.
- The extent to which software vendors supporting the banking sector realise hackers might circumvent the software licensing mechanisms imbedded in their software.
- The extent to which the banking sector realises that hackers could use system resources and storage space for their own illegal purposes.
- The extent to which the banking sector realises that hacker tools and “how to” guides are freely available on the Internet.
- The extent to which the banking sector realises that, increasingly, hackers are pursuing a profit motive.
- The extent to which hackers who engage in terrorism could directly or indirectly affect the banking sector.

Hacking response
- The extent to which the banking sector can detect hacker attacks, even when these are trivial in nature.
- The extent to which the banking sector can recover from a significant and damaging hacker attack. This includes the flexibility built into the banking sector’s business continuity management (hereafter BCM) or DRP plan, to cater for these events.
- The extent to which banking sector acknowledges that hacking is closely related to cybercrime, with numerous illegal cybercrime activities also perpetrated by hackers.
- The extent to which social engineering activities might be successful against the target in the banking sector.
- The extent to which software vendors supporting the banking sector have formulated a response to incidents, which may lead to circumvention of copyrighted software.

3.14 CHAPTER SUMMARY

The literature review conducted in this chapter suggests that the origins of hacking can be traced back to the 1970s, when it referred to individuals with a compulsive interest in programming. During the early years, hacking was associated with positive aspects of computing. But, today, hacking is generally associated with criminal activity, resulting in hacking being regarded negatively as the act of breaking into a system.
Even though this generalisation will apply throughout this thesis, this chapter delved further into the meaning and nature of hacking. Firstly, this chapter considered six different profiles of hackers: script kiddies, crackers, über hackers, black hat hackers, white hat hackers and grey hat hackers. The profiles revealed that hackers differ in two important respects: their skills level and ethical viewpoint. Importantly, these variations will lead to different levels of threat to organisations from hacking depending on the skills set and the ethical viewpoint of the hacker. As regards the acquisition of hacking skills, this chapter provided a glimpse into the accessibility of hacker skills. As regards their ethical viewpoint, this chapter provided an extensive discussion on the range of motives hackers might have, again pointing to the difficulty of using one strategy to address the threat of hacking. In order to consider the meaning and nature of hacking, this chapter went on to document the steps found in a common hacker methodology as well as to look at the basic tools and technologies needed to launch a successful attack.

The chapter also identified several weaknesses that facilitate successful hacking attempts. Weaknesses associated with physical access, logical access, software and hardware vulnerabilities, the inherent risk associated with global interconnected networks and human fallibility all facilitate and lead to successful hacker attacks.

A comprehensive discussion of hacker techniques, ranging from non-technical social engineering techniques, to advanced techniques, such as buffer overflows and race conditions, has also been undertaken. This chapter highlighted that web attacks are a distinct category of hacker techniques, with a broad range of techniques existing in this form of attack. It is important to note, furthermore, that hackers will often make use of the simplest of techniques, such as social engineering, to break into an organisation. This is why organisations will find it challenging to protect themselves against hacker attacks. The chapter also highlighted the close relationship between hacking and cybercrime. Increasingly, hackers are joining professional crime syndicates to profit from illegal activity. This adds an additional layer of complexity to the threat posed by hackers.

The detailed discussion summarised above provided a range of perspectives on the meaning and nature of hacking, and presented a clear picture of the complexities that are associated with the threat. However, given the importance of attending to the threat from a corporate governance point of view in this thesis, hacking was further analysed. By using a deductive approach, it was concluded that hacking might be termed an event on the one hand and a risk on the other hand. As regards hacking as an event, it was concluded that the event would be the result of a risk or risks that would be exploited and from a time
perspective refer to an event that has occurred at present. The event of hacking would be best reacted to through detective controls. As regards hacking as a risk per se, the picture changes in that the risk of hacking refers to a future event that will be addressed via preventative controls. The extent to which detective and preventative controls should be put in place will depend on the extent to which hacking is regarded as a threat.

The discussion in this chapter detailing the significance of hacking in the business context, and specifically its significance in the financial services industry, has provided clear evidence of the importance of hacking in the business environment. Finally, based on the detailed information presented in this chapter, examples of the effect of hacking are provided in order to offer further clarity on what the consequences of hacking are for organisations.

Given that it has been established on the one hand that hacking may be a risk, and on the other hand an event that is the consequence of a risk or number of risks that have been exploited, as well as the prominence of hacking in the business context, the interaction between hacking and risk in the business context must be explored before the responses to hacking can be detailed.
CHAPTER 4

Hacking within the context of business risk

4.1 INTRODUCTION

The highly motivated and elusive nature of hackers poses a threat to many organisations. Hackers present a significant challenge, which needs to be considered from a business risk perspective.

Chapter 3 investigated the meaning and nature of hacking and concluded that hacking may be seen either as a risk, or as an event which is the result of a risk or risks being exploited. Irrespective of which interpretation of hacking is pertinent at any particular time, the fact remains that the concept of risk is key to any response to hacking, since it has been established that hacking is a prominent threat in the business context. Therefore, the concept of (business) risk and the integration between it and hacking must be considered in detail, as the success of any business is intertwined with the risks associated with it. After all, in order for a business to achieve its goals, a clear understanding is required of the business risks that accompany it, which in turn enables it to put appropriate and adequate measures in place to address threats. King II provides clear perspective on the role that risk plays in business (IoD, 2002:76):

Enterprise is the undertaking of risk for reward. A thorough understanding of the risks accepted by a company in the pursuance of its objectives, together with the strategies employed to mitigate those risks, is thus essential for the proper appreciation of the company’s affairs by the board and stakeholders.

The integrated nature of IT in business and the resulting risks are also further emphasised by the King III Report (IoD, 2009b:16):

… the emergence and evolution of the internet, ecommerce, on-line trading and electronic communication have also enabled companies to conduct business electronically and perform transactions instantly. These developments bring about significant risks and should be well governed and controlled.

Consequently, this chapter will start by defining business risk and its components. Thereafter, the characteristics of the chosen components of business risk will be discussed. Given the fact that hacking finds itself within IT, a detailed discussion of IT risk will be
incorporated therein. The outcome of this discussion will lead to the identification of IT risk themes and control objectives, which will form the basis for the discussions that follow. Lastly, the chapter concludes with a discussion of the interaction or integration between each business risk component, hacking and IT risk.

4.2 DEFINING BUSINESS RISK

Section 3.11 highlighted the point that it is difficult to define the concept of risk. Allied to this is the complexity of providing a single definition for business risk. However, given the importance of corporate governance principles in this thesis, it will be useful to approach the discussion of (business) risk from the perspective of King II and King III.

As King II is applicable to all “banks, financial and insurance entities as defined in the various legislation regulating the South African financial services sector” (IoD, 2002:20), the application of the risk categories in King II is even more relevant given the application of this study to the banking sector and financial services organisations in general. King II is emphatic in its viewpoint that the total process of risk management is in the remit of the board of directors (IoD, 2002:30). Interestingly, King II does not contain a reference to the term “business risk” or indeed ERM. Rather, King II uses the term “risk management” and states that a risk assessment should address exposure to at least the following risks (IoD, 2002:31):

- Physical and operational risk.
- Human resources risk.
- Technology risk.
- Business continuity and disaster recovery.
- Credit and market risk.
- Compliance risk.

King III is silent on a definition of business risk and does not offer a single list of risks. King III takes a different view, which is evident from the following (IoD, 2009b:77):

Risk assessments should not adopt a conceptual view or limit itself to a fixed list of risk categories.

In principle, however, King III supports risk management in general (IoD, 2009b:73). To that effect, throughout the King III text, several risks are discussed, including:
• Sustainability risk (IoD, 2009b:11, 13, 77).
• Environmental matters / nature (IoD, 2009b:11, 12, 23).
• Strategic risk (IoD, 2009b:15, 64).
• IT risk (IoD, 2009b:16, 64, 82, 83, 85, 87).
• Operational risk (IoD, 2009b:16, 64, 74).
• Competitive risk (IoD, 2009b:24).
• Ethics risk (IoD, 2009b:25).
• The risk of losing key employees (IoD, 2009b:51).
• Financial / financial reporting risks (IoD, 2009b:64).
• Fraud risk (IoD, 2009b:64).
• Business continuity (IoD, 2009b:78, 83, 120).
• IT legal risk (IoD, 2009b:85).
• Compliance risk (IoD, 2009b:90, 91, 115).
• Reputation (IoD, 2009b:100).

In the context of this thesis, however, it is important to narrow the risks down to key business risks (similar to the risks defined in King II) to facilitate the discussion and links with IT risk. When taking King II’s defined categories of risk as a base (viewed by implication as business risks), it becomes necessary to confirm that these categories are aligned to other definitions of business risk.

4.2.1 Business risk viewed from corporate governance codes

When considering corporate governance codes, few of the prominent codes contain guidance as to the scope or categories of risk that should be considered. For example, codes in the USA, United Kingdom, Germany and the Organisation for Economic Co-operation and Development (hereafter, OECD) are silent on risk categories that should be considered (USA, 2002; OECD, 2004; Financial Reporting Council, 2006; Government Commission, 2010). However, the seventh principle in the Australian corporate governance code focuses on recognising and managing risk. That code states that all material risk must be considered in implementing a risk management strategy, and that the risks that should be considered may include, but are not limited to, operational, environmental, sustainability, compliance, strategic, ethical conduct, reputation or brand, technological, product or service quality, human capital, financial reporting and market-related risks (ASX Corporate Governance Council, 2007:32).
4.2.2 Diverse views of business risk in literature

Cognisance must be taken of other diverse views on business risk found in the literature. For example, Grey and Shi view business risk as the uncertainties related to unique business drivers. According to them, the business drivers which influence business risk include the economic environment, customer demand, changes in technology, and legal and regulatory changes. They also indicated that business risk is difficult to quantify and qualitative assessments thereof are often based on intuition (Grey & Shi, 2005:4). Another view is that business risk is the assumptions, parameters and targets underlying a particular business initiative. These attributes are regarded as the driving factors behind the success or failure of the business initiative. A business will “seek to earn rewards through taking risks” (Olsson, 2002:33). According to Sungard (2008), the organisation should always attempt to manage these uncertainties through its formal risk management processes, as opposed to fallible business instinct. Sutcliff and Donnellan (2006:194) describe business risk as “a prime indicator of business volatility and is defined as the risk of adverse outcomes due to competitive pressures and/or poor decisions concerning strategy, products, markets and structures”. However, Sutcliff and Donnellan (2006:61-62) only see business risk as part of ERM, together with financial risk management, business risk management, operational risk management and event risks management. They define ERM as “the monitoring and management of financial and non-financial risk across an enterprise’s portfolio of assets in support of its strategic objectives” (Sutcliff & Donnellan, 2006:61). So, in considering the literature on risk, it may well be more appropriate to consider the concept of ERM rather than business risk alone, given the pre-eminence of the former term in business literature.

ERM is defined as follows by the Committee of Sponsoring Organizations of the Treadway Commission (hereafter COSO) (2004:2):

Enterprise risk management is a process, effected by an entity’s Board of Directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

COSO further stated that ERM seeks to achieve objectives in four categories: strategic, operations, reporting and compliance (COSO, 2004:3).

Yet another view taken from the literature is that of De la Rosa, who describes the link between business risk and enterprise risk as the evolution of risk management towards a
portfolio or entity-wide enterprise risk approach that recognises that risks are interrelated. He classifies business risk into different types, as presented in Table 4.1 (De la Rosa, 2006:10).

Table 4.1 Business risk types (De la Rosa, 2006:10)

<table>
<thead>
<tr>
<th>• Safety and health issues.</th>
<th>• Economic development.</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Competitive issues.</td>
<td>• Merging technology.</td>
</tr>
<tr>
<td>• Industry-related factors.</td>
<td>• Political events.</td>
</tr>
<tr>
<td>• Environmental matters.</td>
<td>• Reputational issues.</td>
</tr>
<tr>
<td>• Internally sourced risks.</td>
<td></td>
</tr>
</tbody>
</table>

Considering business risk in an integrated or enterprise-wide manner, Shah (2005:49-51) defines numerous risks that could be identified as risks which may threaten the objectives set by the board of directors. Interestingly enough, given the focus of this thesis, Shah did not identify IT risk as a particular risk component, but he did identify the following risks (Table 4.2):

Table 4.2 Business risk from an enterprise-wide perspective (Shah, 2005:49-51)

| • Market risk. | • Competitor risk. |
|                | • Legal risk.      |
| • Credit risk. | • Political risk.  |
| • Weather risk.| • Natural hazard.  |
| • Operational risk. | • Property risk.  |
| • People risk. | • Intellectual capital risk. |

Grey and Shi (2005:9-10) provide a value chain risk taxonomy (Figure 4.1), which can be used as a consistent framework for managing an organisation’s enterprise risks. In this framework, IT risks (termed “systems risk”) are included as a component of operational risk.

4.2.3 Business risk views from banking-related sources

Given the significance of hacking in financial services organisations in the contexts of the proposed empirical work, it is also important to consider banking-related sources on risk. The South Africa Banks Act (Act No. 94 of 1990) deals with the management of risk as part of the governance responsibilities of the board of directors of a bank in the regulation titled “Process of corporate governance”. It places the onus on the board of directors to implement an effective risk management strategy, for the daily management of risks encountered in the banking environment (RSA, 1990:Regulations relating to Banks.III.38.1-.3). The various risks that should be monitored are listed in Table 4.3.
Table 4.3 Risks managed by banks on a daily basis (RSA, 1990:Regulations relating to Banks.III.38.1-.3)

<table>
<thead>
<tr>
<th>Enterprise Risks</th>
<th>Noncore Business</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core Business Risk</td>
<td>Recurring Risk</td>
</tr>
<tr>
<td>Value Chain Risk</td>
<td>Event Risk</td>
</tr>
<tr>
<td>Operational Risk</td>
<td></td>
</tr>
<tr>
<td>Systems</td>
<td>Market Risk</td>
</tr>
<tr>
<td>Policies</td>
<td>Credit Risk</td>
</tr>
<tr>
<td>Procedures</td>
<td>Tax Risk</td>
</tr>
<tr>
<td>Processes</td>
<td></td>
</tr>
<tr>
<td>People</td>
<td></td>
</tr>
</tbody>
</table>

Chibayambuya (2007:2-23) points out that the South African Reserve Bank (hereafter SARB) focuses on all of the risks defined by the Banks Act, increasing banking institutions’ regulatory responsibilities. Consequently, banks are required from a compliance perspective to manage and mitigate various business risks.

4.2.4 Identifying common business risks

The views presented above reflect the diverse views on business risk and its components. In order to confirm that the risk categories presented in King II are in line with categories of business risk presented in a range of sources such as those presented above, a critical analysis is presented in Table 4.4. Business risk types as defined by a number of sources are listed together to identify commonalities. Table 4.4 illustrates that the categories of risk (by implication, business risks) as set out in King II are common to many interpretations of the categories of risk, and can therefore provide a sound basis for the discussion on business risk. By listing the various business risk types discussed in Table 4.4, commonalities between the various sources can be identified. The risks were ranked according to the number of times they have been selected in the sources used.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational risk</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technology / IT / Systems</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Market risk</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance risk</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credit risk</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>People / Human resources risk</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>S</td>
<td></td>
</tr>
<tr>
<td>Environmental matters / natural hazard</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reputational issues</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Political events / risk</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strategic</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reporting</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical risk</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business continuity and disaster recovery</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safety and health issues</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Competitive issues</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Industry-related factors</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internally sourced risks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Economic development</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weather risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulatory risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Competitor risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legal risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Property risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intellectual capital risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Value chain risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recurring risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Solvency risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>Liquidity risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>Currency risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>Interest-rate risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>Counterparty risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>Sustainability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>Ethics risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>Product or service quality</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>Policies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>Procedures</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>Processes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>Tax risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
</tbody>
</table>

**Key:**
- **X**: Applicable risk
- **S**: Categorised as a sub-risk
- **Risk type selected at least 5 times (including King II and sub-risks)**
- **The risks as per King II**
- **Risk type selected at least 4 times**
- **Risk type selected at least 3 times**
Sub-risks have been marked with an “S”, whilst other risks have been marked with an “X”, also receiving priority over sub-risks. The risks defined by King II were highlighted in dark orange, for visible reference. Where risks have been selected five times and more, the cell tables have been highlighted in bright green. Where risks have been selected four times and more, the cells have been highlighted in light green.

Operational and IT risk have been highlighted by six sources, emphasising the importance of those risk categories. Market risk, compliance risk and human resource risk have been highlighted five times, whilst credit risk and environmental matters have been selected three times. From Table 4.4, it is evident that operational, IT, market, compliance, credit and human resource risk (all risks recognised by King II) are also referenced by other sources and therefore common risk categories.

Further to the above, it has already been highlighted in sections 2.1 and 2.6 how significant corporate governance is in the context of this study. Although, arguably, King III should take precedence in this discussion and does emphasises the importance of governing risk (IoD, 2009b:73), the fact is that King III does not provide a definitive list of business risks. Consequently, it provides no definitive starting point for the discussion of business risk in this thesis. It follows that King II, a “national benchmark for corporate governance” in South Africa, provides useful guidance on risk management practices (Van Tonder, 2006:13, 16). King II emphasises that organisations do not only have to manage these business risk types, but also need to disclose how these risks are being managed as part of their disclosure responsibilities (IoD, 2002:31). Many organisations have aligned their business risk and reported those risks in their annual reports to be in line with the requirements set out by King II. Although King III states that an organisation should not limit itself to a fixed list of risks (IoD, 2009b:77), the risks highlighted by King II remain significant in today’s business environment.

If it is further considered that as organisations might continue to report on these business risks, they will remain relevant, also within the context of King III. Therefore, the business risks defined by King II would be of primary consideration. In the context of this study, the King II risk types should be recognised as essential business risk types, supported by other writers, as listed in Table 4.4. Physical risk, business continuity and disaster recovery, which are business risks defined by King II, have not been highlighted in Table 4.4. However, given the importance of the King II code from a corporate governance perspective, as well as the relevance of the three risk types in this study, they will be included as common risk categories. As Table 4.4 shows, environmental matters were listed four times in the sources;
however, since it is not recognised by King II as a risk category and is not directly relevant to this study, it will be excluded from the risk categories.

Another business risk to consider, although highlighted only three times in Table 4.4, is reputational risk. The Economist Intelligence Unit (2005:5, 19) identified reputational risk as the biggest risk amongst 12 other business risks (from a risk management survey conducted in October 2005, with 269 senior risk managers who participated). Reputational risk could be an organisation’s downfall: an example of this is the demise of the once reputable organisation Arthur Andersen after the Enron scandal (O’Rourke, 2004). It is events such as these that have focused management attention on reputational risk. In addition, as noted in the previous paragraph, organisations have to disclose how they manage business risks. A breach in any of the business risk types will also affect the reputation of an organisation. In particular from a hacker breach perspective (noted repeatedly in sections 3.9.6 and 3.12.6 and 3.13) and how that will be perceived by clients, shareholders and the general public, reputational risk is important in the context of this thesis and will be included in the discussion of business risk.

In Table 4.4 evidence is provided of how the risk categories in King II provide an appropriate basis for the discussion of business risk, which are representative of a general classification of the categories or components of business risk. Reputational risk has been added, due to the relevance of this risk type in the context of this thesis. The basic nature of each of these risk categories will be discussed in the section that follow. Most of the business risks identified should be applicable to a lesser or significant extent to organisations of any size; however, exceptions may exist. The final list of business risks considered in this thesis is:

- Physical risk.
- Operational risk.
- Human resources risk.
- Technology risk.
- Business continuity.
- Disaster recovery.
- Credit risk.
- Market risk
- Compliance risk.
- Reputational risk.
Thematological research questions

Based on the literature review above, the following thematological research questions can be defined:

**Business risk**
- The extent to which those targeted in the banking sector agree with the completeness of the risk categories as a representation of business risk.

**Corporate governance**
- The extent to which each of the risk categories is considered in the banking sector from a corporate governance risk management perspective.

### 4.3 THE CATEGORIES OR COMPONENTS OF BUSINESS RISK

#### 4.3.1 Introduction

Even though there are differing views on the categories or components of business risk, the risks included in King II has been proven to provide a balanced view when compared to many other views as explained in section 4.2. The basic definitions for and characteristics of the categories of risk set out in King II will now be presented to create the platform for the discussion around the link between hacking and each risk category. As regards which of the risk categories should be discussed first, it must be noted that there is a degree of overlap between all the risk categories that will be touched on within some of the discussions of the basic characteristics and then expanded on later when the link between the risk categories and hacking is discussed. Therefore, this discussion will follow the sequence used in King II (IoD, 2002:31).

#### 4.3.2 Physical risk

The first category of risk that must be addressed as part of good corporate governance is physical risk (IoD, 2002:31). Various views on it are found in the literature. One interpretation of physical risk is that it relates to the exposure of an organisation’s physical assets to acts of vandalism or theft (IMS Risk Solutions Ltd., 2003:28; Young, 2006:15, 17). Hoffman (2002:48) views “physical asset risks” as the risk to an organisation’s business processes and key facilities, either due to the unavailability of physical assets, or due to improper maintenance of physical assets. A similar view is shared by Esterhuysen (2003:15). Hoffman (2002:49) further expounds that physical risk could also be attributed to physical damage due to natural (for example, floods) or manmade disasters (for example, terrorism). The response to physical risk is regarded by many as an organisation’s first line of defence.
against a range of risks and threats (Etsebeth, 2003:38). Physical security mechanisms must therefore ensure protection against a range of threats, including fire, floods, humidity, earthquakes and loss of power supply (Herrmann, 2002:28; Etsebeth, 2003:38; Suduc, et al. 2010:43). Physical risk could also lead to a loss of privacy and identity theft (Larson, 2009:70). The literature also suggests that physical risk could relate to unauthorised access to an organisation’s building or premises, which may lead to theft or damage to assets. Even though this unauthorised access may come from outside the organisation, the risk of inappropriate staff access must also be addressed, such as through different access levels, to provide additional protection for some of an organisation’s assets (Whitman & Mattord, 2008:46).

Within the context of this thesis, it is important to consider how physical risk relates to technology. Historically, from a technology perspective, physical risk associated with computer hardware has always been important, even before the advent of interconnected networks. Then, IT operations were restricted to physical rooms or data centres. Due to the complexities associated with operating these systems and the significant capital injection that went into the purchasing of the systems of the 1960s and 1970s, only limited access was allowed, with some form of physical access control in place (Van Biene-Hershey, 2007:660-661, 666). The bulky equipment was housed in the EDP department, and was not accessible to other members of staff, as explained in section 2.2. Now, computers, servers, networks and related IT equipment are found pervasively across organisations, and physical access risks to all parts of an organisation must therefore be addressed. The nature of open shared workspaces is such that users can access their data at numerous points, as opposed to using only a dedicated PC (McLean, 2003:68). The risk that a perpetrator can obtain access to a premises, and then obtain unauthorised access to a network, advertently or inadvertently tampering with physical equipment such as servers or stealing media that contains confidential data must be addressed (Herrmann, 2002:28; Whitman & Mattord, 2008:46). Physical risk is further exacerbated by the mobility of technology. Employees could remove multi-gigabyte storage devices from the physical boundaries of the organisation, exposing the organisation to theft in multiple locations. Technology could also extend the network environment beyond the organisation’s physical boundaries, through the use of wireless technologies. As explained in sections 2.5 and 3.8.3, employees who enable remote connection functionality on their cellular phones and PDAs present an opportunity for unrestricted access to personal information, including authentication details that might be stored on the mobile device (Herzog, 2006:75; Yarberry, 2006:1303).

As regards the detail of King II, it must be noted that the code lists physical risk only as a
component of risk management (IoD, 2002:80). Even though it could have been expected that physical risk would be addressed in the chapter on “Safety, Health and the Environment” (IoD, 2002:114-121), or in the chapter on “Information Technology” (IoD, 2002:147-150), no further reference is made to physical risk. Similarly, King III has a whole chapter that deals with the governance of risk (IoD, 2009b:72-80), yet does not include a single reference to physical risk.

Lastly, apart from the direct theft of assets and data resulting from physical risk, it is important to consider the indirect consequences of physical risk, which is the reputational risk that may be associated with a breach in physical security. Particularly as regards the theft of data, any such a report that reaches the public domain could inevitably lead to a loss of consumer trust (Ross, 2008:9).

**Thematological research questions**

Based on the literature review above, the following thematological research questions can be defined:

**Business risk**
- The extent to which attention is paid to physical risk in the banking sector.
- Recognition of the most significant challenges in respect of managing physical risk in protecting IT equipment and resources in the banking sector.
- The extent to which physical risk is addressed from a technology point of view in the banking sector.
- The extent to which physical risk is managed beyond the brick-and-wall confines of banks.

**4.3.3 Operational risk**

Operational risk can also be defined in a number of ways. It is argued that prior to 2001, organisations focused on credit, market, interest rate and foreign exchange risks, whilst other risk categories did not receive much attention. With the introduction of ERM, organisations started adding other risk categories under the operational risk category (Kloman, 2005:1). Bostander (2007:27) argues that operational risk was not clearly defined in the past, which led to the inclusion of many financial and non-financial risks under the category of operational risk. Literature suggests that an earlier definition of operational risk by the Basel Committee, before the introduction of Basel II, saw it as “deficiencies in information systems or internal controls” (as quoted by Power, 2005:579). With the introduction of Basel II, it has been defined as “the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events” (as quoted by Power, 2005:584).
The Basel Committee on Banking Supervision (as quoted by TransConstellation, 2007a:12) defines operational risk as: “A risk not related to the way a firm finances its business, but rather to the way a firm operates its business”. Very similar to Basel II, the Bank for International Settlements (hereafter Basel, 2001:17) defines it as “the risk that deficiencies in information systems or internal controls, human errors or management failures will result in unexpected losses”. Crouhy, Galai and Mark (2001:37) extend the earlier interpretation by the Basel Committee, and define it as the risk related to the execution of a business. It is the potential for losses, due to “inadequate systems, management failure, faulty controls, fraud, and human error”.

Further to the above, Alexander (2001:191) argues that operational risk is multi-dimensional. Firstly, he views it as “all potential losses that are not directly attributable to credit or market risk”. Secondly, he is of the opinion that it is composed of strategic risk (potential losses due to the failure in the organisation’s defined strategy) and operational failure risk (people, processes, technology and external dependencies). It is important to note that all the abovementioned definitions contain one or more elements of the four areas which form part of many definitions or interpretations of operational risk: people, processes, systems and external factors, which appear to be the most common interpretation of operational risk (Smit, 2008:5).

The literature review suggests, however, that operational risk is believed to be a diverse category of risk, when compared to other risk types, such as interest rate risk (Esterhuysen, 2006:19). According to the ITGI, the Basel II definition of operational risk includes legal risk, but excludes strategic and reputational risk, albeit predominantly from a banking perspective (ITGI, 2007d:10, 19). Grody, Hughes and Mark (2008:140) note that operational risk can be divided into categories focusing on expected losses and unexpected losses. The organisation will be able to absorb expected losses; however, it needs to plan carefully for unexpected losses. Power (2004:30) argues that operational risk is aimed at taking risks which may seem unknown and “incalculable” and changing them to be noticeable and manageable. This illustrates the complexity of defining and managing operational risk.

Some authors define additional categories within operational risk. Jackson and Carey (2006:1614), for example, identified the categories business interruption, privacy, marketing, processes, physical assets, technology infrastructure, legal and human resources. Alexander (2001:227) has identified additional risks, such as “write-downs, loss of recourse, restitution, legal liability, regulatory and compliance (including taxation)” and “loss of or damage to assets”. The Institute of Risk Management (hereafter IRM), the Association of
Insurance and Risk Managers (hereafter AIRMIC) and ALARM, the National Forum for Risk Management in the Public Sector (2002:3), have defined internal and external drivers for operational risk. The internal drivers are accounting controls, information systems, recruitment and the supply chain. External drivers include regulations, culture and board composition. Esterhuysen (2003:13, 15) identified a number of levels in operational risk, which include people, processes, technical, technological and physical. These levels are also supported by Mbokane (2005:2.15). The Basel Committee has identified the following operational event types: internal fraud; external fraud; employment practices and workplace safety; clients, products and business practices; damage to physical assets, business disruption and system failures; and execution, delivery and process management (ITGI, 2007d:49). In particular from an external fraud perspective, cybercrime, which includes hacking, has been highlighted by the Basel committee (Basel, 2009:20). Nierengarten (2006:24) also recognised cyber threats such as identity theft, credit card fraud, and phishing as operational risks. These examples illustrate the broad range of risks and events that form part of operational risk.

Crouhy, et al. (2001:478-479) split operational risk into two distinct categories: operational failure risk (internal) and operational strategic risk (external), depicted in Figure 4.2.

**Figure 4.2 Two elements of operational risk (Crouhy, et al. 2001:478-479)**

<table>
<thead>
<tr>
<th>Operational failure risk (Internal operational risks)</th>
<th>Operational strategic risk (External operational risks)</th>
</tr>
</thead>
<tbody>
<tr>
<td>The risk encountered in the pursuit of a particular strategy due to:</td>
<td>The risk of choosing an inappropriate strategy in response to environmental factors, such as:</td>
</tr>
<tr>
<td>- people</td>
<td>- political</td>
</tr>
<tr>
<td>- process</td>
<td>- taxation</td>
</tr>
<tr>
<td>- technology</td>
<td>- regulation</td>
</tr>
</tbody>
</table>

Chibayambuya (2007:2-29), Young (2006:12), the Basel (2004:137) and Lam (2003:210) broadly concur with the interpretation in Figure 4.2, as they view operational risk as having four components: people, processes, technology (or systems) and external factors. In turn, each of these four components is defined in Table 4.5.
Table 4.5: Definition of operational risk components (own interpretation)

<table>
<thead>
<tr>
<th>Operational risk component</th>
<th>Definition of risk component</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Process risk</strong></td>
<td>The risk of losses due to the operational failure of business processes (Young, 2006:16).</td>
</tr>
<tr>
<td><strong>People risk</strong></td>
<td>“The risk of loss caused intentionally or unintentionally by an employee.” (Young, 2006:13)</td>
</tr>
<tr>
<td><strong>Systems risk</strong></td>
<td>The risk of loss due to failure, breakdown or disruption in technology or data processing. It could be further extended to losses incurred due to theft of data or information, or failure to meet intended business IT needs (Hoffman, 2002:36). Lam (2003:21) argues that systems risk include “systems availability, data integrity, systems capacity, unauthorised access and use, and business recovery from various contingencies.”</td>
</tr>
<tr>
<td><strong>External factors</strong></td>
<td>External factors are beyond the control of an organisation, yet influence the operational factors. Examples are economic and political activities, terrorist threats and, industrial and labour union strikes (Young, 2006:17).</td>
</tr>
</tbody>
</table>

In section 4.3.1 it was pointed out that there are overlaps between the risk categories to be discussed. In terms of operational risk, this overlap is specifically evident when it comes to systems risk and its link with technology or IT risk. For example, Young (2006:9, 15) includes the following events under system risks (some of which were discussed in section 3.13 as the outcome or effects of hacking): system failure, theft of data, security breaches, late delivery of software projects and implementation failure, insufficient systems capacity, weak data integrity, failure of equipment, destruction of systems and obsolescence of systems. Systems risk is so closely associated with technology that authors even substitute the word “system” with “technology”. For example, Fishkin uses this substitution in his discussion of operational risk (Fishkin, 2006:107). He therefore views “systems risk” as being synonymous with “technology risk”. Fishkin focuses specifically on IT-related technologies in his discussion of technology risk. He argues that technology risk could be imbedded in the development and use of IT systems. Indeed, Fishkin (2006:400) also views “technology risk” as being synonymous with “IT risk”. Writers such as Pareek categorise technology risk as a component of operational risk (Pareek, 2011:26).

In a dissertation titled “The Management of Operational Risk in South African Banks”, Esterhuysen (2003:15) argues that technology risk relates closely to IT risk. She goes on to point out that technology risk includes failure of systems, due to external disruption, failure to conduct system maintenance, software issues, outdated software, system interfacing issues and poor system development projects. Maria (2009:197) also discusses IT risks as part of the technology risk component and specifically includes hacking as a security issue related to technology risk.

From a technology risk perspective, in its operational risk management benchmark tool for
the banking industry, TransConstellation divides the characteristics of operational risk into internal and external factors as depicted in Figure 4.3 and classifies technology under both (TransConstellation, 2007b:6).

The effect of operational risk on reputational risk also needs to be considered. Kloman (2005:1, 2) considers the impact of operational events on the reputation of an organisation. He considers that continued communication with key external stakeholders is important in managing the reputational risk of the organisation. Glaessner, Kellermann and McNevin (2002:17) identified inadequate electronic security as an operational risk and points out that it relates to reputational risk. External factors, such as hacking, are a key contributor to operational risk events, and may increase the organisation’s reputational risk.

Figure 4.3 Operational Risk Management (ORM) process view (adapted from TransConstellation, 2007b:6)

Even though operational risk is listed as a risk category in King II, the code makes limited reference to operational risk in the chapter on risk management and in the appendix on directors’ legal duties (IoD, 2002:80, 187). Although King II discusses various operational processes (for example, reporting and accounting processes) and people issues (for example, transformation and black economic empowerment), these are not aligned with or
discussed in the context of the concept operational risk (IoD, 2002:122, 133). The King III Report highlights that the complexities associated with IT systems could cause operational risk (IoD, 2009b:16). These complexities require audit committees to be duly informed of significant operational risk issues (IoD, 2009b:64).

<table>
<thead>
<tr>
<th>Thematological research questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Based on the literature review above, the following thematological research questions can be defined:</td>
</tr>
</tbody>
</table>

**Business risk**
- The extent to which attention is paid to operational risk in the banking sector.
- The significance of technology in the banking sector, and more specifically IT, from an operational risk perspective.
- The extent to which operational risk is also addressed from a technology point of view in the banking sector.
- The extent to which hacking is considered as a risk from an operational risk perspective in the banking sector.
- The extent to which the banking sector uses systems risk to overlap with technology or IT risk.

### 4.3.4 Human resource risk

A key component of any organisation is its human resources. Views by several authors are considered in this section, taken from books and accredited journal articles covering human resource issues. Human resource risk can be defined as “the challenges or business improvement opportunities dealing directly with the people or employees in an organization” (Leisy, 2009:8). Leisy continues by reflecting on the risk factors associated with human resource risk, which includes talent management and succession planning; regulatory compliance; rewarding for performance; and training and development. He also mentions that the “tone at the top” and ethical values of the organisation have a role to play in mitigating human resource risk (Leisy, 2009:8).

From an operational risk perspective, Esterhuysen (2003:13) discusses people risk in the context of employment, and identifies employee error, employee misdeed, employee unavailability and employment malpractice as factors which could increase an organisation’s people risk. She defines people risk as follows (Esterhuysen, 2003:13):

People risk is the risk due to a human (employee) error, a lack of expertise and fraud, including a lack of compliance with existing procedures and policies.

Several factors contribute to human resource risk, such as discrimination, violence in the workplace, harassment and unfair dismissal. Human resource risk is an “emotionally
charged" risk, closely linked to the actions, words and deeds of the organisation’s employees. It is believed that human error is inextricably part of human resource risk. The employer might be held responsible for the unlawful actions of its employees (Hinton, 2003:58). It is argued that an employee leaving the organisation should be considered a risk (Stephen, 2001:25-29). Bornman (2004:82-83) also concurs that employees leaving should be regarded as a risk and emphasises that the loss of productivity and poor organisational communication adds to human resource risk. Employees seek job satisfaction, personal growth, reward and recognition, the presence of which will lead to organisational loyalty (Leblanc, 2009:186). However, the lack thereof will increase human resource risk.

Employee safety during disaster scenarios, employee injury, employee litigation and organisational inefficiencies leading to loss of productivity, should be considered as key contributors to human resource risk (Luper, 2002:60). Ernst & Young (2008:56) conducted a survey into the current global trends related to human resources risk, by interviewing more that 150 Fortune 1000 global executives (95 from the USA and 65 from other countries globally). According to the survey, human resource risk ranks among the top three business risks (IT and market risk being the others). The effects of globalisation, underpinned by advances in technology, also need to be considered. More and more organisations’ workforces are being mobilised (such as working from home), exposing the organisations to bigger risks (Ernst & Young, 2008:61).

Sanchez (2010:49) has indicated that the general lack of skilled IT resources and the inability to provide them with attractive job benefits, combined with staff turnover, may also by implication increase human resource risk. Sanchez goes on to argue that this also has an impact on the performance of an organisation, which ultimately increases business risk. It is further suggested that advances in technology may also increase human resource risk, where employees have to adapt to new technologies and IT systems being introduced into their work environment. A possible strategy to manage this risk is to allow only incremental change and resolve emanating human resource issues as they occur (Koning, 1997:363-364). This risk should be closely monitored and managed through training programmes (Young, 2006:14). Organisations are also at risk when hiring new IT personnel, in particular IT graduates with no prior work experience. They might not have the required knowledge and experience to maintain the organisation’s systems, increasing the organisation’s human resource risk and the risk of hacking. The literature suggests that it is not only technical skills that might be inadequate. IT personnel often lack the required soft skills, to interact with their fellow colleagues and work in teams. Organisations have to invest substantially in appropriate training for these individuals, as a means of managing the human resource risk.
IMS Risk Solutions views human resource risk as the critical dependency on people as part of operations. It argues that the human resource component is often taken for granted, by not focusing on their wants and needs (IMS Risk Solutions, 2003:32). Moeller (2007:25) groups human resource, employee turnover, performance incentive and training risks all under people risks. Considering the obvious relationship between human resource risk and people risk that forms part of operational risk, the nature of human resource risk may be better understood if the discussion is linked to people risk from an operational perspective. In this regard, Young (2006:12-13) defines people risk as an operational failure caused by the behaviour of staff members. He goes on to provide three factors contributing to people risk:

- **Error** – This relates to human error during transaction processing or failure to follow a defined process.
- **Fraud** – This relates to deliberate actions of staff, in being dishonest or, for example, falsifying records.
- **Dependency on key staff** – This relates to over-reliance on a key individual or group of staff members, without having succession planning in place.

Fishkin (2006:180-181) indicates that there are various possible events which could lead to people risk, and which need to be monitored as part of the risk management process, as listed in Table 4.6.

<table>
<thead>
<tr>
<th>Events which could increase people risk (Fishkin, 2006:180-181)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Overtime.</strong></td>
</tr>
<tr>
<td><strong>Crises in the workplace.</strong></td>
</tr>
<tr>
<td><strong>Financial losses.</strong></td>
</tr>
<tr>
<td><strong>Unreasonable demands from other staff.</strong></td>
</tr>
<tr>
<td><strong>Uninformed bosses.</strong></td>
</tr>
<tr>
<td><strong>Inflexible leadership.</strong></td>
</tr>
<tr>
<td><strong>Uncooperative subordinates.</strong></td>
</tr>
<tr>
<td><strong>Work environment.</strong></td>
</tr>
</tbody>
</table>

Similar characteristics can be associated with people risk, such as inadequate training, lack of segregation of duties, lack of succession planning and dishonesty (Smit, 2008:86).

Apart from being listed as a risk category in King II, the code refers to human resource risk in the chapter on risk management (IoD, 2002:80) even though no detail is provided. Further, section 4 of King II, dealing with integrated sustainability reporting, provides some information on human capital where it denotes the value of an organisation’s employees and
the contribution they make towards the organisation. It recognises that the lack of human resources with the appropriate level of skill or experience could have a detrimental effect on the organisation (IoD, 2002:127-129, 132). This detrimental effect has not only a direct impact on an organisation, but also a potential reputational loss if customer satisfaction suffers as a result. King III does not address people risk specifically. The concept “people” is discussed in the context of sustainability and the triple bottom line (a reference to how organisations operate via “people, profit and planet”) (IoD, 2009a:22; IoD, 2009b:128).

**Thematological research questions**

Based on the literature review above, the following thematological research questions can be defined:

**Business risk**
- The extent to which attention is paid to human resources risk in the banking sector.
- Realisation of the technology-related factors or events, which may have a positive or negative effect on human resource risk in the banking sector.
- Whether human resource risk is also addressed from a technology (or IT) point of view in the banking sector.
- The extent to which there is an understanding that human resource risks could increase the risk of hacking in the banking sector.

**4.3.5 Technology risk**

Technology risk is a reality for organisations making use of some form of technology or IT to conduct business. This relationship between business and technology risk has sparked new debate, as evidenced in the professional guidance provided by the IIA (The IIA, 2008:6):

> Technology exists to further a business goal or objective. The failure of technology to perform as intended (i.e., technology risk) may result in or contribute to a business risk – the risk that business goals and objectives are not achieved effectively and efficiently.

This sections starts out by defining technology risk. This is followed by a discussion of the effect new and outdated technologies have on technology risk. From the literature review perspective, it is then argued that there is an overlap between technology, systems and IT risk. This leads to a discussion on technology risk from a corporate governance perspective. This is followed by a discussion of IT risk prior to and after the advent of interconnected networks. IT risk is then discussed from a number of sources, with the goal of identifying IT risk themes (and control objectives).
4.3.5.1 Definition and characteristics of technology risk

Various definitions of technology risk are found in the literature. Technology risk can be defined as “the risk of a potential failure of a given technology combined with the incremental risk that technology can add to an existing process” (Holmquist, 2008:41). Holmquist explains that “incremental risk” may include increased complexity, misuse and the cumulative effect of increased processing speed, which may lead to propagation of errors. Holmquist also argues that technology is “deeply embedded” in all operations, which shows a strong relationship with operational risk. Also in the context of this thesis, the effect technology has on an organisation and how it should be managed can be expressed as follows (Holmquist, 2008:41):

The industry has allowed technology risk to be managed largely on an intuitive and reactive basis for many years; however, as technology continues to become more complex and businesses become more dependent on it, a much more proactive, structured approach to managing risk must be used.

Technology risk can also be defined as (Luecal, 2009:40):

The failure to realize the desired benefits from implemented technology due to lack of product completeness or stability, an ineffective implementation, or the failure to completely integrate technology functionality, work flow processes and employee responsibilities.

In a book titled Operational risk management: The practical application of a qualitative approach, Young does not define technology risk. However, he identifies several characteristics which can be associated with technology risk. He points out that poorly designed systems could lead to complexities and vulnerable systems. This creates the risk of possible security breaches. Rapid changes in technology and, more specifically, IT could lead to outdated systems or systems obsolescence. This in turn might result in regular system or equipment failures. As a consequence, significant skills requirements for technology might be created, increasing the organisation’s technology risk (Young, 2006:14-15).

Other writers have identified similar characteristics for technology risk, such as system failures, programming errors, information risk and telecommunications failures (Crouhy, et al. 2001:487), while IMS Risk Solutions (2003:30-31) lists several characteristics associated with technology risk, as presented in Table 4.7.
Table 4.7  Technology risk characteristics (IMS Risk Solutions, 2003:30-31)

<table>
<thead>
<tr>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>The absence of research or development.</td>
</tr>
<tr>
<td>Inability to lead by innovation.</td>
</tr>
<tr>
<td>Outdated products and methods.</td>
</tr>
<tr>
<td>Issues of reliability.</td>
</tr>
<tr>
<td>Poor replacement of equipment.</td>
</tr>
<tr>
<td>Power failures.</td>
</tr>
<tr>
<td>Outdated hardware and software.</td>
</tr>
<tr>
<td>Threats posed by viruses and hackers.</td>
</tr>
<tr>
<td>Non-existent back-ups.</td>
</tr>
<tr>
<td>Corruption of data.</td>
</tr>
<tr>
<td>Poor maintenance.</td>
</tr>
<tr>
<td>Incompetent technical staff.</td>
</tr>
<tr>
<td>Poor security of IT.</td>
</tr>
</tbody>
</table>

The study by Esterhuysen (2003:14) indicates that technology risk can be attributed to poor information systems and IT system malfunctions. Another writer is of the opinion that users are contributors to technology risk (Brancik, 2005:414). If users do not follow the organisation’s policies and procedures, the confidentiality, integrity and availability of information might be affected. Maizlish and Handler (2005:278) identified the following technology risk factors, as presented in Table 4.8.

Table 4.8  Technology risk factors (Maizlish & Handler, 2005:278)

<table>
<thead>
<tr>
<th>Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security.</td>
</tr>
<tr>
<td>Availability.</td>
</tr>
<tr>
<td>Architecture.</td>
</tr>
<tr>
<td>Business processes.</td>
</tr>
<tr>
<td>Applications.</td>
</tr>
<tr>
<td>Development.</td>
</tr>
<tr>
<td>Disaster recovery.</td>
</tr>
<tr>
<td>Complexity.</td>
</tr>
<tr>
<td>Information.</td>
</tr>
<tr>
<td>Performance.</td>
</tr>
<tr>
<td>Integration.</td>
</tr>
<tr>
<td>Feasibility.</td>
</tr>
<tr>
<td>Maturity.</td>
</tr>
<tr>
<td>Existing assets.</td>
</tr>
</tbody>
</table>

The significance of preventative and detective controls required to address technology risk is an important consideration in the context of this thesis and will be further explored during the discussion of technology and IT risk. The significance is captured by the following quote (Philee & Philee, 2010:11):

Consideration of technology risks and the deliberate examination and implementation of technology controls should be ingrained within the day-to-day operations of our organizations. Effective internal control over information technology and all technical resources is essential to fully realizing and leveraging our technology resources.

4.3.5.2  The impact of outdated technology on technology risk

Outdated technology could be a drawback for organisations in a highly competitive marketplace, leading to non-achievement of their defined business objectives (Connolly, 1999:15). Larger organisations might have the funding and skills available to upgrade to new technology, in contrast with smaller organisations. Outdated technology could also be costly to maintain, complex to interface or update, which increases technology risk (Connolly,
Outdated technology not only hampers the growth of the organisation, but could also affect employee morale, due to the frustrations of dealing with a slow and tedious system. This will clearly increase human resource risk. Vulnerabilities in older systems can easily be exploited by hackers to gain access to the organisation’s network and data (Fishkin, 2006:181). A high likelihood of failure of these older systems will increase business continuity risk, increasing business risk.

4.3.5.3 The impact of new technology on technology risk

Technology risk is also evident when new technology is introduced for the first time in an organisation. The literature suggests that new technology introduced into an organisation might be unknown. Skilled personnel who have the knowledge to comprehend, implement and maintain the new technology might be unavailable or non-existent. An organisation could underestimate the complexity involved in implementing the new technology and fail to launch the appropriate change management process to support the implementation. The time it takes to assimilate the new technology might also be underestimated. The implementation approach might be complex, involving multiple departments and multiple interfacing systems and processes (Stephens, 1994:1, 2, 11). Gupta and Karahanna (2003:3) also share a similar view in terms of the inherent complexity associated with new technology.

It is suggested that newly acquired systems often require modification, to ensure that they function as intended within the organisation. Unfortunately, this introduces more vulnerabilities, new security challenges and possible control failures. Clearly, this will not help the organisation to achieve its business objectives. Management must seek ways of effectively managing the risks forthcoming from these new technologies (Young, 2006:14; Ross, 2009:9-10). Similarly, advances in technology could create pressure on organisations to keep up to date with the latest developments in technology (Young, 2006:15). In particular, in the field of IT, there is continuous evolution of new technology. It is not always practical for the organisation to keep up with the latest developments in IT. Organisations will have to determine for themselves how up to date they want to be with the latest technological advances.

New technology from an IT perspective will have unknown vulnerabilities associated with it. One such example cited from the literature is wireless technology. Wireless networks have many business benefits, such as reduced cost and ease of deployment. Nonetheless, wireless networks increase technology risk due to the inherent risks associated with this
technology, as discussed in sections 3.8.3.3 and 3.8.6. Poor implementation of wireless networks could lead to successful security breaches by hackers. This might affect not only the organisation’s compliance risk, due to the possible exposure of confidential client data, but could also increase the organisation’s reputational risk, due to media exposure of the security breach (Pickard, 2007:339). As another example, Internet banking applications are also under a constant threat of being attacked by hackers or criminal syndicates. The use of untested technology to enhance Internet banking applications increases technology risk (ISACA, 2010c:93, 96). The complexities are often misunderstood by IT staff, introducing vulnerabilities which are exploited by hackers. This threatens the stability of business solutions being offered to clients, which increases business risk.

The background section of the Basel Committee on Banking Supervision’s “Sound Practices for the Management and Supervision of Operational Risk” discusses four technology risks faced by banks as a result of the growing sophistication of financial technology, increasing bank’s operational risk profile (Basel, 2003:1):

- With more reliance placed on highly automated and integrated technology, it increases the potential for repeating similar errors, which could lead to total system failure.
- E-commerce solutions introduce new risks, in particular system security issues, and the possibility of internal or external fraud.
- Large-scale acquisitions, mergers, de-mergers and consolidations test the agility and adaptability of integrated systems.
- Since banks are large-volume service providers, continued maintenance of internal controls and backup systems is required.

It is therefore evident from the literature above that new technology increases an organisation’s technology risk.

### 4.3.5.4 Overlap between the concepts technology risk, systems risk and IT risk

Based on the definitions and characteristics considered in this thesis, it is submitted that technology risk is a collective term for risks associated with advances (or the lack thereof) in technology in the broader sense of the word and includes IT risk as a sub-component. This view is supported by a number of authors:

- “Just think of technology and start to list the things that might go wrong which could prevent computer systems being available to operators when they needed them – system crashes, data backup failure, data corruption, slow retrievals, search facilities
not working, etc.” (Olsson, 2002:31)

- “...fast developments in the field of technology ... while most of the world is still trying to understand the operational risks involved in the Internet.” (Schönfeldt, 2000:26)

- “Technology risk. Information technology continues to play a central role in running organizations.” (Fishkin, 2006:355)

- “To minimize technology risk ... business audiences ... need to have the same level of confidence as they do with their current IT infrastructure and applications ...” (Evans, 2002:48)

Similar to the technology risk characteristics presented by Young (2006:14-15) as discussed in section 4.3.5.1, Fishkin (2006:355) argues that IT is the origin of many diverse issues, related to hardware, software, organisational strategy, people and system design. He is also of the opinion that due to the continued advancement and innovation in IT, new risks will emerge, which need to be understood. Fishkin’s opinion, if read together with the discussion of operational risk in section 4.3.3, emphasises the link between systems risks, technology risk and IT risk which are evident through the following examples:

- “Systems. Almost all services depend on information technology systems. Problems can arise from the corruption of data stored on the systems, whether accidental or deliberate, for example, programming errors and fraud.” (Young, 2006:9)

- “System risk. As technology has become increasingly necessary, in more and more areas of business, operational risk events due to systems failures have become an increasing concern.” (Lam, 2003:213)

- Risks relating to systems risk include flaws in system design, weaknesses in programming or methodology, system failures or breakdown in communications (Du Preez, 2003:28).

- “Systems risk is the risk of loss arising from computer failures or system infiltration, and the risk of breakdown of other systems.” (Alexander, 2001:207)

The effect of IT on the scope of technology risk is clearly evident from the discussion presented by Chapman in his book titled *Simple tools and techniques for enterprise risk management*. He is of the opinion that organisations might be faced with inadequate technology governance and in particular IT governance, which may lead to a lack of alignment of IT to business objectives. He is also concerned that organisations might be faced with the risk of inadequate protection against viruses, hacking and loss of confidentiality of information (Chapman, 2006:264).
The view that technology brings with it new challenges is shared by Merna and Al-Thani in the following quote (Merna & Al-Thani, 2005:175): “The use of more technology will increase the threat of hacking, virus attacks and cyberterrorism.” A similar view is shared by Bonnette (2002), who points out that technology introduces threats and vulnerabilities. Both internal threats, such as insiders, and external threats, such as hackers, have to be considered.

4.3.5.5 Technology risk from a corporate governance perspective

From a corporate governance perspective, King II addresses technology risk twice. In section 2 dealing with risk management, technology risk is listed as an area for risk assessment, and the issue is also included in Appendix III on directors’ legal duties (IoD, 2002:80, 187). King III does not address technology risk specifically. The King III Report refers to technology from an IT governance perspective, as is evident in the following quote (IoD, 2009b:82): “IT governance should focus on the governance of the information as well as the governance of technology.”

In respect of IT and IT risks, King II and King III are more comprehensive. King II makes several references to IT in general (IoD, 2002:151, 262). It also emphasises the importance of IT in achieving risk-based principles of validation, security, integrity, availability and continuity (IoD, 2002:84). Section 5 of chapter 4 deals with IT matters impacting corporate governance aspects, such as internal control systems and reporting (IoD, 2002:147-150), and includes three important recommendations – set out in Table 4.9 (IoD, 2002:150).

<table>
<thead>
<tr>
<th>Table 4.9</th>
<th>King II recommendations for IT (IoD, 2002:150)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• “Information technology has had a profound effect on processes within organisations. Accordingly, boards need to ensure that the necessary skills are in place to ensure that their responsibilities in respect of internal control systems are adequately discharged.</td>
<td></td>
</tr>
<tr>
<td>• Potential benefits that result from using technology to improve reporting and transparency should be embraced.</td>
<td></td>
</tr>
<tr>
<td>• Directors need to be mindful of the implications of blurred organisational barriers that arise as a consequence of an e-business, to the extent that these result in their governance responsibilities extending beyond the traditional corporate boundaries. They need to ensure that the same levels of governance are applied in the companies with which they integrate along the supply chain.”</td>
<td></td>
</tr>
</tbody>
</table>

King II highlights the point that IT has a significant impact on six areas of corporate governance: internal control systems, reporting, fiduciary implications, business, technology and the cost/value relationship. Of particular importance is the impact of IT on business and
technology. The views from King II on these two areas are presented in Tables 4.10 and 4.11.

**Table 4.10  King II impact of IT on business (IoD, 2002:149)**

- "The introduction of e-business initiatives has resulted in a fundamental change in the way that business is conducted, with a greater degree of integration of processes in the supply chain than traditional systems ever allowed. This change has implications for internal control systems, as well as statutory compliance with legislation, for example the Competition Act."

**Table 4.11  King II impact of IT on technology (IoD, 2002:149)**

- "Technology has had a fundamental impact on the way in which business is conducted and businesses are measured. All of the responsibilities to stakeholders that are part of good governance have a pronounced role in IT companies.
- Typically these organisations have traded at a significant earnings multiple because of their perceived growth potential. Employees are often attracted to these businesses with comparatively low fixed income because of the same growth expectations. Many stakeholders in these organisations do not have a full understanding of the true opportunities and threats facing the organisation. Consequently, the importance and the basic tenets of good governance is particularly significant.
- Management needs to be completely honest and transparent in reporting on organisational results and prospects."

King III takes an even stronger stance on the significance of IT, dedicating an entire chapter to the governance of IT. There is a clear focus on IT risk in King III, already from the introductory parts of the King III Report (IoD, 2009b:16). King III also expresses the concern that "the internet, ecommerce, on-line trading and electronic communications" have increased the number of risks and threats associated with IT (IoD, 2009b:16). These new delivery channels introduce risks organisations did not have to deal with in the past. The King III Report also recommends that audit committees ensure that IT risk from a financial reporting perspective has been adequately addressed (IoD, 2009b:64). Other references to IT risk are listed in Table 4.12.

**Table 4.12  References to IT risk in the King III Report (IoD, 2009b:82, 83, 85, 87)**

- "The IT governance framework should include relevant structures, processes and mechanisms to enable IT to deliver value to the business and mitigate IT risk."
- "Effective IT frameworks and policies, as well as the processes, procedures and standards that these involve, should be implemented with the view to minimise IT risk, deliver value, ensure business continuity, and assist the company to manage its IT resources efficiently and cost effectively."
King III highlights that an organisation’s IT governance policies and frameworks should include mechanisms to deal effectively with IT risk, towards the achievement of the organisation’s objectives. The day-to-day significance of IT risk is expressed as follows (IoD, 2009b:82):

IT is essential to manage the transaction, information and knowledge necessary to initiate and sustain a company. In most companies, IT has become pervasive because it is an integral part of the business and is fundamental to support, sustain and grow the business. Companies should understand and manage the risks, benefits and constraints of IT.

King III further spells out the responsibilities of management from an IT governance perspective, such as defining the processes, procedures and standards which will ultimately mitigate and manage IT risk (IoD, 2009b:83). In particular, IT risk should be managed and monitored via the organisation’s risk management process (IoD, 2009b:85) and the risk committee should have a strong role to play in ensuring that IT risks are adequately managed (IoD, 2009b:87). The King III Report includes seven key governance principles defined specifically to address IT (as presented in Table 2.2).

There is no doubt that King III acknowledges the significance of IT risk and the role it plays from a corporate governance perspective. Furthermore, when it is considered that IT risk closely links with and influences other risk types, such as financial risk, regulatory risk, business risk, strategic risk and security risk (Schlarman, 2009:27), it becomes clear that IT risk does have a pervasive and “cross-functional” impact on business (Fischer, 2009a:30). The board of directors needs to consider and manage it as one of their key business risks. They also need to acknowledge the implications hacking may have in increasing IT risk within the organisation.

Given the prominence of IT risk within this thesis, it will be explored further through an overview of the main focus areas of IT risk prior to the advent of interconnected networks. Secondly, it will be examined by reflecting on the IT risk associated with interconnected networks, where after some perspectives will be presented on the meaning and scope of IT risk from a variety of sources. Overall, the size and complexity of the organisation and the
applicability of the IT risks discussed need to be considered.

4.3.5.6 The main focus areas of IT risk prior to the advent of interconnected networks

Before the advent of open systems and interconnected organisation-to-organisation networks (discussed in chapter 2), IT risk was localised within organisations to a large extent. In these closed systems, IT risk and security mostly centred around two issues. Firstly physical access to systems and data, and secondly risks related to the integrity of data.

In respect of physical access to systems, in the 1960s the number of locations that had to be protected was limited to special rooms where all IT equipment was housed. IT operations mostly resided in central EDP departments (discussed in section 2.2). Tape libraries had to be secured and tape registration procedures were introduced to restrict access to sensitive program information stored on tape (Van Biene-Hershey, 2007:660-661). Access control varied from standard lock and key procedures to pin-pad access. In other words, a great deal of the IT risk emphasis was related to the general business risk category of physical risk.

Regarding the integrity of data, the overarching goal is the completeness, accuracy, timeliness and validity of information. Internal control procedures such as hash totals, batch totals and validation checks are performed manually and on an increasingly automated basis. Considering the business risks selected for this thesis as set out in section 4.2, these goals are also related to wider business risks, specifically operational risk and compliance risk.

As the use of databases became the norm, automated integrity and validation checks, as well as the use of exception reporting, became the minimum standard. However, at that time, the number of IT risks was limited and, to a large extent, did not get the attention afforded to other risk categories that appeared to be more important, such as credit risks and market risk.

Today, the same automated techniques are still used, but with increased efficiencies. However, given the advances in IT, these techniques can now address only a portion of IT risks.
4.3.5.7 New focus areas of IT risks associated with the advent of interconnected networks

As discussed in sections 2.3 and 2.4, a significant advancement in IT during the 1980s and 1990s was the interconnectedness of IT systems. Since the early 1990s, open access to computer networks introduced the need to further refine access control. Whereas physical access control and single location logical access control were crucial prior to that time, access control now implied logical access via distributed locations that extended beyond the boundaries of organisations. As systems opened up and transactions were initiated via networks, encryption techniques to secure data over transmission channels and firewall software protecting internal networks from external network connections (Van Biene-Hershey, 2007:678) became the order of the day, thereby raising the technical abilities of those interested in technology in general. Although environments became “harder to control”, the technology required to protect against IT-related risk also became more sophisticated. New technologies such as wireless computing, mobile devices and the integration of audio and video into computing underscores the importance of matching new technologies and risks with risk strategies (ITGI, 2007c:12).

From a business risk perspective, the common assets related to IT such as computers, servers etc. can still be managed in an effective way with basic techniques such as access control. However, when it comes to data and control over data, which is a crucial asset in business today, the picture has evolved dramatically. Perhaps one of the best descriptions of the current position is that by Boni, who lists the following challenges (Boni, 2008:5-6):

- The mobility of users is of concern at a business risk level through “the convergence of ubiquitous connectivity and evermore powerful portable handheld devices”.
- Network environments are no longer discrete environments with defined boundaries.
- New access pathways into networks have opened up rapidly through means of mobile broadband connectivity.
- As organisations frequently outsource core activities, the rules of access are blurred, as it is becoming increasingly difficult to distinguish between “outsiders” and “insiders” who need access to the organisation’s business applications for multiple purposes.
- The proliferation of the use of small but powerful mobile devices that may be used to copy large portions of organisational data has become virtually impossible to control.
- The accessibility that individuals have to devices such as cellular telephones that are used for private purposes, but also for business, whether to diarise business meetings or to download e-mails, has created privacy problems and IT security problems in
many organisations. These devices are not company assets, and users may install any software on these devices, which may increase the likelihood of a virus or Trojan infection in the company data that is stored on the same device.

- Organisations also find it increasingly difficult to find the right balance between allowing employees the freedom to be creative, by using the full functionality of software applications, while at the same time maintaining IT security. For example, many organisations bar their employees from installing unauthorised computer software on their computers, while, if given the opportunity to experiment, there may very well be open source software that could be used to the benefit of the organisation.

These complexities listed above introduced new vulnerabilities and IT risks, while the criminal element started exploiting these vulnerabilities and IT risks. Boni describes the significant and increasing threat of cyber criminals and cyber spies as follows (Boni, 2008:6):

In the 21st century, hackers seem bent on ways of parasitic extraction of value from targeted organizations that raise the least amount of concern and, thus, reaction from the ‘hosts’.

In this thesis, a glimpse into the definition and scope of IT-related risks from varied sources is required, so to underscore the prevalence and pervasiveness of risks associated with IT and the broad business impact it may have. It is important to note that research conducted by Alter and Sherer (2004) and Worrel and Bush (2007) has indicated that it is not possible to provide a definitive definition for IT risk. All four writers argue that IT risks are situational and depend on the outlook and position of the person identifying the risks. Therefore, rather than trying to provide a definitive list of IT risks, a broad overview of IT risk from various sources will be given. This overview of IT risk from a variety of sources will show that, due to the pervasive impact of IT on business, the varied number of technologies and the diverse number of issues and complexities which can be associated with IT, it is problematic to provide a definitive list of IT risks. However, this overview will enable some conclusions as to typical risk areas or themes that are found in IT environments.

The methodology followed in the sections on IT risk that follows involves an extensive literature study, providing an overview of IT risk. The sources referenced include textbooks, journals and articles on information security, IT risk management, auditing and IT auditing and a number of sources from professional audit and IT audit organisations. These are subject areas where one is most likely to find credible views on IT risk and the risks associated with hacking. This will aid in the discussion of the link between the various business risks, IT risk and hacking. These are also subject areas which will be considered,
when providing an effective response to the risk of hacking, which will be covered in chapter 5.

It is not only IT risk, but also control objectives which will be considered in the sections that follow. Control objectives are “desired conditions" management wishes to achieve (Vallabhaneni, 1989:96-97). Baldwin, Beres, Shiu and Kearney (2006:54) argue that an organisation’s risk management process should define a set of control objectives aimed at mitigating risk. In this section, the focus is on IT risk, which management is trying to avoid or mitigate. It follows that when controls to mitigate IT risk are designed, management will set control objectives they wish to achieve. Therefore, in the context of this thesis, control objectives are the opposite of IT risk.

**4.3.5.8 Discussion of IT risk from information security sources**

IT risk features prominently in the field of information security. The sources used in this section have a strong focus on information security and IT risk. Information security is typically concerned with the confidentiality, integrity and availability of information (Bornman, 2004:14; Etsebeth, 2003:40; McCumber, 2005:29; Jordan & Silcock, 2005:13; Conklin, 2008:2), which can also be regarded as control objectives.

Considering IT risk from an information security perspective, the following definitions are presented: “It’s the potential for an unplanned event involving a failure or misuse of IT to threaten an enterprise objective" (Westerman & Hunter, 2007:1). “The adverse effects that would result if a threat were to be actualised, or if a vulnerability were to be exposed or exploited" (Smith, 2000:10).

In his book titled *Strategic Information Security*, Wylder, who is cited at least 25 times (Google, 2010e) by writers such as Wu and Saunders (2005), Tabor (2009) and Syamsuddin and Hwang (2010:95), identified four IT risk categories which deal with strategic information security. He considers these four IT risks as overarching in nature (Wylder, 2004:79-81):

- **Infrastructure risk** deals with risks such as the type of infrastructure, lack of capacity planning, protection of infrastructure. He also groups external risks, such as hackers and terrorists, under this category.
- **Vendor risk** deals with risks such as a lack of vendor support, frequency of software updates, lack of support for older releases of vendor products and vendors going out of business.
• **Technology risk** deals with risks such as choosing the correct technology, the technology life cycle and risks associated with selecting emerging software.

• **Information risk** deals with the threats and risks associated with information as an asset of the organisation.

In the book titled *Information Assurance: Managing Organizational IT Security Risks*, it is noted that information security management requires risk management to guard against the “expected loss of accountability, access control, confidentiality, integrity, or availability from an attack or incident”, due to the IT risks presented in Table 4.13 (Boyce & Jennings, 2002:25).

### Table 4.13 IT risks threatening information security (Boyce & Jennings, 2002:25)

| • Sabotage.                          | • Fraud.                  |
| • Interference.                     | • Embezzlement.           |
| • Denial of service.                | • Misuse.                 |
| • Espionage.                        | • Lack of segregation of duties. |

Harris defines several IT risks from an information security perspective, in the Certified Information Systems Security Professional (hereafter CISSP) Exam Guide (Harris, 2005:65):

• **“Physical damage**: Fire, water, vandalism, power loss, and natural disasters.

• **Human interaction**: Accidental or intentional action or inaction that can disrupt productivity.

• **Equipment malfunction**: Failure of systems and peripheral devices.

• **Inside and outside attacks**: Hacking, cracking, and attacking.

• **Misuse of data**: Sharing trade secrets, fraud, espionage, and theft.

• **Loss of data**: Intentional or unintentional loss of information through destructive means.

• **Application error**: Computation errors, input errors, and buffer overflows.”

The chapter by Lynne, titled “Toward an integrated theory of IT-related risk control” in the book titled *Toward an integrated theory of IT-related risk control* (Lynne, 2000:169), cited at least 15 times (Google, 2010f), touches on several IT-related risks forthcoming from the information security literature, such as information security project failures, operational failures, security breaches, reputational damage and strategic risk. Peltier (2001:193), in the book *Information security risk analysis*, lists several IT risks (associated with the corresponding IT risk type or control objective), to be considered as part of a formal information security risk analysis process, summarised in Table 4.14 below.
Table 4.14  IT risk type and risk descriptions considered as part of an information security risk analysis (adapted from Peltier, 2001:193)

<table>
<thead>
<tr>
<th>IT Risk Type</th>
<th>IT Risk Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrity / Confidentiality / Availability</td>
<td>Unauthorised internal or external access / unattended workstation.</td>
</tr>
<tr>
<td>Integrity</td>
<td>Improper editing routines for data entry functions or external feeds.</td>
</tr>
<tr>
<td>Integrity</td>
<td>Timeliness of external feeds.</td>
</tr>
<tr>
<td>Integrity / availability</td>
<td>Program bugs.</td>
</tr>
<tr>
<td>Integrity</td>
<td>Lack of change or version control.</td>
</tr>
<tr>
<td>Integrity / Availability</td>
<td>Viruses.</td>
</tr>
<tr>
<td>Integrity</td>
<td>Corrupted database.</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Lack of software management.</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Lack of user awareness associated with information classification.</td>
</tr>
<tr>
<td>Availability</td>
<td>External feeds, mainframe, servers of WAN unavailable.</td>
</tr>
<tr>
<td>Availability</td>
<td>Lack of application DRP, backups or plan to restore.</td>
</tr>
</tbody>
</table>

Similar to Peltier, Conklin lists the following information security threats, which can also be considered IT risks (Conklin, 2008:3):

- Data loss from hardware malfunction.
- Data loss from accidental deletion or human error.
- Data loss through theft.
- Data misuse by insiders.
- Accidental or deliberate data modification.
- System interference.
- Natural or manmade disasters.

As stated at the beginning of this section, information security is often described by the three information security elements: confidentiality, integrity and availability. It seems that from an information security perspective most IT risks are diverse, yet relate to these three elements, which closely resemble control objectives. It is another means of identifying and categorising IT risks.

4.3.5.9 Discussion of IT risk from IT risk management sources

This section will show that IT risk also features prominently in the field of IT risk management. The discussion starts with the widely referenced Westerman and Hunter (Fischer, 2009b:25; ISACA, 2009:23, 98; Google, 2010d) in their book titled IT risk: Turning business threats into competitive advantage, who define IT risk as “the potential for an unplanned event involving a failure or misuse of IT to threaten an enterprise objective ... An
IT risk incident has the potential to produce substantial business consequences that touch a wide range of stakeholders” (Westerman & Hunter, 2007:1). They do not provide a classification of specific aspects of IT risk that need attention, but they do provide a view of the objectives of IT systems through a framework (referred to as the “4A” framework) for the management of IT risk presented in Table 4.15. These can be seen as examples of control objectives.

Table 4.15 Key concepts for the management of IT risk (Westerman, 2005:1; Westerman & Hunter, 2007:23)

<table>
<thead>
<tr>
<th>Availability</th>
<th>Ensuring that the systems are up and running, and could recover from disruption.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>Allocating appropriate access to data and systems, to valid and authorised users.</td>
</tr>
<tr>
<td>Accuracy</td>
<td>Produce correct, timely and complete information to stakeholders, including management, staff, customers, suppliers and regulators.</td>
</tr>
<tr>
<td>Agility</td>
<td>The ability to change or adapt systems, without compromising on cost and speed.</td>
</tr>
</tbody>
</table>

In addition, in the book titled *Information Technology Security & Risk Management* it is noted that IT risks can arise internally for an organisation (strategic and operational risks) and also externally (regulatory, environmental, market and technological risks). In particular, technological risks such as Internet “spoofing”, hacking, telecommunications failure and e-commerce leading to market share losses could be external risk factors that an organisation needs to identify timeously (Slay & Koronios, 2006:14). Rainder, Snyder and Carr (1991:130, 131) identified similar risks, categorising them under authorised and unauthorised physical and logical threats, and recognising that they can originate from both internal and external sources.

Worrell and Bush define IT risk as “the risk that an organization’s information systems will not adequately support the organization in achieving its business objectives, sufficiently safeguard its information resources, or deliver accurate and complete information to its users” (Worrell & Bush, 2007:2). There is a strong focus on information security in this definition. Worrell and Bush used 13 risk factors in their research to test the perceptions of participants on IT risk. These risk factors are presented in order of priority in Table 4.16 (Worrell & Bush, 2007:5).

Table 4.16 IT risk factors (Worrell & Bush, 2007:5)

1. Lack of organisational alignment between business and IT.
2. Unauthorised information access.
3. Information quality.
4. Interdependencies between systems.
5. Weak change management.
8. Technical complexity.
9. Problematic interfaces between systems.
10. Difficulty integrating software from vendors and subcontractors.
11. Malicious software.
13. Unauthorized physical access to hardware and processing environment.

A special publication titled “Risk Management Guide for Information Technology Systems” issued by NIST defines IT-related risk as the probability of a threat attacking a weakness and the impact of this on the organisation. The following factors which could lead to IT-related risks, resulting in legal implications or losses in production, have been identified (Stoneburner, Goguen & Feringa, 2002:E.2):

- The unauthorized disclosure, modification or destruction of information.
- Unintended errors and omissions.
- Disruption of IT operations due to manmade or natural disasters.
- Lack of due diligence in the implementation and operation of IT systems.

The IT risk management report by Symantec (cited by Abram, 2009:53), in its discussion of IT risk management, provides a framework which can be used by organisations to analyse their IT risks. This framework is presented in Figure 4.4 (Symantec, 2007:7).

**Figure 4.4 IT risk framework (Symantec, 2007:7)**

Symantec (2007:7) argues that IT risks can originate from four areas:

- **Security risk**: The unauthorized modification, access to or use of information. Clearly, this could include the threat of hackers.
- **Availability risk**: The inability to access information due to natural disasters or failure of systems.
- **Performance risk**: Loss of operational productivity due to systems, applications or...
employees who are underperforming.

- **Compliance risk:** Failure to meet regulatory or organisational policy requirements.

Again, the diverse nature of IT risk is apparent from the IT risk management sources consulted.

### 4.3.5.10 Discussion of IT risk and control objectives from auditing sources

In the context of this thesis, IT risk as defined by auditing sources is of particular importance. Several auditing books have been reviewed in preparation for this section; however, only some of them discuss IT risk. Essentially, three groups of role players can be distinguished: internal audit, external audit and audit committees. Internal and external audit provide assurance to the board of directors and shareholders, the former focusing on effectiveness of internal control and the latter focusing on the accuracy of financial statements (IoD, 2009b:93, Smith, 2003:16). The audit committee is responsible for ensuring a coordinated effort between the various assurance providers (such as internal and external audit), to ensure that all significant organisational risks have been addressed (IoD, 2009b:62). Therefore, IT risk from an audit committee perspective is considered first.

#### 4.3.5.10.1 Views on IT risk from an audit committee perspective

Audit committees are increasingly concerned about IT risk, recognising the importance of IT as an enabler of operations, finances and services (Scharf, 2007; KPMG International, 2007:5). Audit committees could play an active role in either attending IT governance committees, or by closely aligning with such committees, to ensure all regulatory and compliance issues have been dealt with (Nolan & McFarlan, 2005:106). A public company audit committee member survey conducted by KPMG during 2007 indicated that IT risk was the fourth highest priority for audit committees, with a third of respondents (282 directors who serve on audit committees in the USA) not being satisfied with the IT oversight provided by audit committees (KPMG International, 2007:7, 16). In order to fulfil their corporate governance responsibilities, audit committees are required to have a deeper understanding of IT risk and how IT vulnerabilities relate to IT risk (The IIA, 2006:1). Audit committees look to internal audit to provide them with assurance on how effectively management deals with IT risk. A survey conducted by the company Protiviti during 2009 identified industry trends in relation to internal audit needs and capabilities. A total of 700 executives and professionals, mostly in the internal audit field, were interviewed. IT risk was ranked by the survey as the highest area of required technical competency, illustrating the perceived significance of IT
risk from an internal audit perspective (Protiviti, 2009:2, 18).

Research into the effectiveness of Top 40 JSE-listed South African audit committees conducted by Marx (2008:82-83, 465) highlighted the need for audit committees to take ownership of IT governance and to have adequate knowledge of IT and IT risk, due to the increased reliance on IT and the significance of IT risk in today’s business environment. His research indicated that only 1 out of Top 40 South African organisations provided disclosure of IT risk in their annual financial statements (Marx, 2008:408, 440) and only 47% (16 out of 34) of audit committees had adequate expertise to review IT risks (Marx, 2008:444).

During the 7th Annual Audit Committee Issues Conference, hosted by KPMG’s Audit Committee Institute in the USA, IT risks associated with cloud computing and the loss of sensitive company data were highlighted as a key concern. Only 19% of participants, consisting of 120 audit committee members and business leaders, received feedback related to issues associated with cloud computing (KPMG LLP, 2011:A1). The challenge for audit committees is to stay abreast of the latest developments in IT, as well as the associated risks.

4.3.5.10.2 Views on IT risk and control objectives from an internal audit perspective

When considering views from an internal audit perspective, the views of the IIA have particular significance. The IIA has been at the forefront of providing guidance to internal auditors worldwide (The IIA, 2010d). Recognising the significance of IT and the effect it has on the control environment, the IIA has increased its focus on IT risk and technology issues (Moeller, 2008:120) and has provided guidance through the issuing of the Global Technology Audit Guides (hereafter GTAG) series, which will be dealt with separately in section 4.3.5.14.2. Internal audit functions therefore have a high focus on the implications of IT risk in their organisations. It follows that views by internal audit on IT risk should be considered.

In a text published by the IIA Research Foundation (hereafter IIARF), the following common types of IT risk have been identified (IIARF, 2009:7.8-7.9):

- Selection risk (selection of IT solutions not aligned with the organisation’s strategic objectives).
- IT development, acquisition and deployment risks.
• System availability risks.
• Hardware and software failure risks.
• Unauthorised physical and logical access risks.
• System reliability and information integrity risks.
• Confidentiality and privacy risk.
• Fraud and malicious actions risk.

The internal audit function is an integral component of corporate governance (IoD, 2002:90) and plays a key role in the mitigation of IT risk. From an internal auditing perspective, the seminal work of Sawyer, Dittenhofer and Scheiner includes the following perspectives on IT. Firstly, it categorises control procedures into three areas (Sawyer, Dittenhofer & Scheiner, 2003:71):

• **General information systems controls** that include computer operations controls, physical and logical security controls, program change controls, system development controls and telecommunications control.

• **Application controls** “that are designed to ensure authorized, accurate, and complete processing of a transaction from input, through processing, to the output of information”.

• **Compensating controls** that “overcome or mitigate a weakness in another application of general control”.

Sawyer, *et al.* (2003:150) further emphasise the importance of the nature of a control as either preventative or detective. As regards data security, Sawyer, *et al.* (2003:559) hold the view that “data may be an organization’s most critical asset”. In this regard, attention must be paid to logical and physical security measures. Sawyer, *et al.* provide four characteristics of an effective data security system (Sawyer, *et al.* 2003:559):

• “Only authorized users have access to data.

• The level of access is appropriate to the need.

• Modifications to data are accompanied by a complete audit trail.

• Unauthorized access is denied and the attempt is reported.”

They also state that there are numerous approaches to data security, but that it must include general and application controls (Sawyer, *et al.* 2003:559). In addition, numerous other IT risks are discussed by Sawyer, such as unauthorised physical access, environmental hazards, unauthorised changes to the operating system, lack of segregation of duties, failure of telecommunications networks and fraudulent changes to production applications (Sawyer,

In a book titled *Managing the Audit Function. A Corporate Audit Department Procedures Guide* by Cangemi and Singleton, which provides guidance on the establishment of an internal audit department, “computer controls” are broken down into general and application controls (Cangemi & Singleton, 2003:111-112). The text also discusses the threat posed by hackers, such as releasing viruses and performing distributed DDoS attacks (Cangemi & Singleton, 2003:123).

In *Brink’s Modern Internal Auditing*, which is already in its 7th edition, Moeller does not discuss IT risk per se, but does discuss IT general controls, such as (Moeller, 2009:382-383):

- Ensuring dependability of processing done by information systems.
- Integrity of data and programs.
- System development and implementation controls.
- Ensuring continuity of processing.

Moeller also highlights that IT systems and data may be affected by threats that can be classified into interruptions, interceptions, modification and fabrication (Moeller, 2009:462). He also discussed other IT risks, such as weak password controls, viruses and other malware, as well as phishing (Moeller, 2009:464-467).

From a comprehensive piece of work commissioned by the IIA (titled “Research Opportunities in Internal Auditing”), the impact of IT on internal auditing has been identified as a research area. From a risk management perspective in particular, Ramamoorti and Weidenmier (2004:320-321) have identified the following IT risks relevant to an e-commerce environment (see Table 4.17):

**Table 4.17 IT risks relevant to an e-commerce environment (Ramamoorti & Weidenmier, 2004:320-321)**

<table>
<thead>
<tr>
<th>• Malware.</th>
<th>• Repudiation.</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Unauthorised access.”</td>
<td>Transaction failures.</td>
</tr>
<tr>
<td>Hackers.</td>
<td>Spoofing.</td>
</tr>
<tr>
<td>Technological obsolescence.</td>
<td>Failures of partners.</td>
</tr>
<tr>
<td>System incompatibilities.</td>
<td>Availability.*</td>
</tr>
</tbody>
</table>

Closely related to the threat of hacking are the following information system risks (Table 4.18) highlighted by Pickett (2010:588), in his book titled *The internal auditing handbook*. 
### Table 4.18 Information system risks (Pickett, 2010:588)

<table>
<thead>
<tr>
<th>Information system risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft of proprietary information.</td>
</tr>
<tr>
<td>Eavesdropping.</td>
</tr>
<tr>
<td>Abuse of Internet access.</td>
</tr>
<tr>
<td>Denial of service.</td>
</tr>
<tr>
<td>Viruses.</td>
</tr>
<tr>
<td>Sabotage of data or networks.</td>
</tr>
<tr>
<td>System penetration.</td>
</tr>
<tr>
<td>Fraud.</td>
</tr>
<tr>
<td>Spoofing.</td>
</tr>
</tbody>
</table>

While management is responsible for defining the organisation’s risk appetite, internal audit is responsible for ensuring the “integrity and completeness of the entire risk management process”, which includes a focus on operational risk, covering technology and IT risk in particular (Alexander, 2001:193).

#### 4.3.5.10.3 Views on IT risk and control objectives from an external audit perspective

External audit firms also extensively focus on technology and IT risk, in both an advisory and assurance capacity (Deloitte Touche Tohmatsu, 2010b; PwC, 2010b; Ernst & Young, 2010). From this perspective, IT risk also needs to be considered from an external auditing perspective. In this section, views are taken from authoritative South African auditing textbooks and other authoritative authors in the auditing field.

The authoritative South African auditing textbook by Marx, van der Watt, Bourne and Hamel, which could arguably be used from an internal and external audit perspective, contains references to standards mostly used by external audit, and consequently will be used here from an external audit perspective. It was written based on the educational requirements of the South African Institute of Chartered Accountants (hereafter SAICA) (Marx, van der Watt, Bourne and Hamel, 2009:v, 9.4). The textbook does not define IT risk per se, but rather places emphasis on the following computer information system risks to reflect on the topic, which is a view largely echoed by Marx, Schönfeldt, van der Watt and Potgieter (2006:114-115):

- Unauthorised access and changes to data and programmes.
- A lack of segregation of duties.
- Unauthorised authorisation via automatically generated transactions.
- A lack of an audit trail, due to the temporary nature of data or the lack of printed documentation.
- Errors in software that could lead to invalid or erroneously processed data.
- Loss of data during data transmission.

Furthermore, Marx, et al. (2009:9.11-9.13) present a discussion of additional risks that
organisations are exposed to in a computerised environment. In this regard, particular mention is made of risks related to the integrity of financial information:

- Unauthorised access and changes to data, transactions and programmes, by external and internal parties.
- The absence of input documentation and the lack of a visible audit trail supporting evidence of authorisation.
- Corruption, duplication, loss or manipulation of data during transmission or as a result of unauthorised network access.
- The lack of segregation of duties or supervision in a decentralised processing environment. Staff may also lack appropriate training.
- System-generated transactions could lead to consistent errors, across numerous systems. Due to high processing speed, errors may go unnoticed.
- Absence of physical output in the form of reports, also leading to less manual review.
- Types of software (purchased versus developed), in particular where there is only a small IT department or hardware used.
- Batch versus on-line processing. Batch processing has additional checkpoints, which might be omitted in an online processing system.
- The effectiveness of the control environment and computerised controls, including potential weaknesses in general and application controls.
- The nature, size and materiality of transactions.
- Dependency and complexity of computer operations, creating a going concern risk.
- Dependency on key staff members, who holds a detailed knowledge of systems and processes.

Marx, et al. (2009:9.13-9.14) go on to list additional IT risks that relate to management’s requirements:

- Risks related to the access to data, including confidentiality, unauthorised use and privacy.
- Business continuity affected by denial of access.
- Computer fraud.
- Availability, completeness and quality of management information.
- The system’s ability to cope with high volumes of transaction.
- IT staff competency.
- Dependence on communication and technology.
- The morale of staff, due to changes in systems and processes.
Marx, et al. (2009:12.8–12.9) also define the following control objectives, which relate to internal controls that could be implemented to address IT risks. A control objective can be seen as the objectives management wishes to achieve with the internal controls (further considered in section 4.3.5.11) being implemented, towards addressing the associated risk (Van Der Watt, 2010). The control objectives are: validity, authorisation, completeness, accuracy, recording, classification and cut-off.

In another South African auditing textbook, Puttick, Van Esch and Kana do not specifically define IT risk on its own. They do however provide the following discussion of IT risks (Puttick, et al. 2007:392):

- The concentration of IT personnel in an IT department could lead to a lack of segregation of duties. It could also lead to a situation where a single individual holds the knowledge of a single application, including its control weaknesses. This individual could use this knowledge to his advantage.
- Master data is stored centrally, increasing the risk of unauthorised access, which in turn may lead to amendments or theft of data.
- A transaction error will be consistently processed until corrected. A programmer who has access to the vulnerable application in question could use this to his advantage, through manipulating the programme in order to benefit him personally.
- Transactions may be entered without supporting documents. Data entry authorisation may be automated, for example automatic granting of credit facilities.
- There may be a lack of visible output of processed transactions.
- Incorrect data capturing may lead to errors in a distributed system, where multiple databases are updated automatically.
- The data and programmes stored on portable media are vulnerable to theft, loss or damage.

Puttick, et al. (2007:409-410) also list risks associated with software applications encountered in a business environment, as presented in Table 4.19.

<table>
<thead>
<tr>
<th>Table 4.19 Risks associated with business software applications (Puttick, et al. 2007:409-410)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weak security.</td>
</tr>
<tr>
<td>Unauthorised access to data.</td>
</tr>
<tr>
<td>Unauthorised remote access.</td>
</tr>
<tr>
<td>Inaccurate information.</td>
</tr>
<tr>
<td>Erroneous of falsified data input.</td>
</tr>
<tr>
<td>Misuse by authorised end-users.</td>
</tr>
</tbody>
</table>
It is important to note that Puttick, *et al.* (2007:477) also recognise that preventative and detective controls are required to address the risks associated with IT. Like Moeller (2007), they divide IT controls into general and application controls (Puttick, *et al.* 2007:473, 476, 477).

In another book, which could also arguably be used from both an internal and external audit perspective, Jackson and Stent (2001:8/9) also distinguish between general and application controls. They list main categories of general controls, which provide an indication of areas of IT risk, which is presented in Table 4.20. With reference to applications, they distinguish between input, processing and output functionality of applications (Jackson & Stent, 2001:8/24).

<table>
<thead>
<tr>
<th>Table 4.20 Main categories of general controls (Jackson &amp; Stent, 2001:8/9)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• “Control environment and security policy.</td>
</tr>
<tr>
<td>• Organisational structure and personnel practices.</td>
</tr>
<tr>
<td>• Standards and standard operating procedures.</td>
</tr>
<tr>
<td>• System development controls.</td>
</tr>
<tr>
<td>• Program change controls.</td>
</tr>
<tr>
<td>• Continuity of operations.</td>
</tr>
<tr>
<td>• Access controls.</td>
</tr>
<tr>
<td>• Documentation.”</td>
</tr>
</tbody>
</table>

In another book, focusing on teaching integrated auditing from a predominantly external audit perspective (although internal auditors can also benefit from this textbook), IT risks are considered from a control objectives perspective, as reflected in Table 4.21 (Hooks, 2011:389).

<table>
<thead>
<tr>
<th>Table 4.21 IT risks addressed through general and application controls (Hooks, 2011:389)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• “Data confidentiality.</td>
</tr>
<tr>
<td>• Data availability.</td>
</tr>
<tr>
<td>• Data integrity.</td>
</tr>
<tr>
<td>• Data timeliness.</td>
</tr>
<tr>
<td>• Date accuracy.</td>
</tr>
<tr>
<td>• IT infrastructure.”</td>
</tr>
</tbody>
</table>

A similar book often prescribed for undergraduate and graduate students, highlights the risks associated with e-Commerce applications, such as cybercrime, viruses, DoS and cyber terrorism. The textbook also recognises the risks associated with “crackers”, and makes specific reference to insiders and the risk they pose to an organisation (Cosserat & Rodda, 2009:595-596). Yet another textbook for students preparing for the Association of Chartered Certified Accountants (hereafter ACCA) exams supports the division of IT controls into application and general controls (Kaplan Financial Limited, 2010:183).

Ultimately, much of what is produced from an IT system finds its way into the financial statements of an organisation. In respect of IT risks associated with the integrity (validity,
completeness and accuracy) of financial information and management’s requirements of an IT system, unauthorised and uncontrolled access, sabotage, corruption of data, possible fraud (Marx, et al. 2009: 9.11, 9.12, 9.13, 9.14), and threats to business continuity feature prominently as risks. Even though these occurrences may result from a number of causes, they can all potentially result from hacking.

4.3.5.10.4 Conclusion on IT risk and control objectives from audit literature

On the whole, the audit literature consulted focuses on IT risks and controls. It is evident that an organisation has to manage and monitor a broad spectrum of IT risks. From the audit literature, the categories general and application controls repeated themselves. In addition, unauthorised access, transaction processes prone to error, and data susceptible to change and deletion are some of the risks which also repeated themselves. All of these could be as a result of hacking.

4.3.5.11 Discussion of internal controls

One of the objectives that management would want to achieve is to mitigate IT risk. In order to mitigate IT risk, management has to implement appropriate internal controls (which include IT and business controls), which are deemed to be effective (IRM, AIRMIC & ALARM, 2002:10). IT controls represent in effect the opposite of IT risk (own deduction). In order to study IT risk from an internal controls perspective, various sources were consulted on COSO, SOX and auditing. In this section, it is argued that IT controls have two dimensions. The first relates to the general nature of controls, divided into general and application controls, the second focuses on the type of controls, which include preventative, detective and corrective controls.

Given that general and application controls are implemented to address IT risk, the concepts are further explored. The text by Moeller, which has been cited at least 19 times (Google, 2010b), provides the following explanation and examples of controls as they relate to general and application controls:

- **General Controls**: Information systems general controls include hardware, software, and administrative processes and procedures which apply to systems and applications in general:
  - **Reliability of information systems processing**. Effective controls need to be imbedded in all information systems operations. The controls have to be customised according to the size and complexity of the system.
o **Integrity of data.** A high level of data integrity should be maintained for all operational applications.

o **Integrity of programs.** Changes to programs should follow a well-defined change control process, to ensure programs operate as intended.

o **Controls of the proper development and implementation of systems.** System development practices should be followed for new and revised systems to ensure minimal vulnerabilities in software code.

o **Continuity of processing.** Disaster recovery and business continuity planning should be in place to ensure uninterrupted operation of business critical applications (Moeller, 2007:297).

- **Application Controls:** Application controls apply to specific business applications, over and above general controls. Examples of application controls include:

  o **Controls of application inputs.** Business applications should have input validation, logical access restrictions, and other controls to limit the risk of unauthorised inputs into the application.

  o **Self-balancing and other financial and data controls.** Applications should have error-checking routines and reconciliation controls, to ensure accurate processing of data.

  o **Application output components.** Controls should ensure that the integrity of application output data is accurate on output reports and correctly filed. This includes protection of data during transmissions or communications with other connected applications (Moeller, 2007:297).

In his book titled *How to comply with Sarbanes-Oxley section 404: Assessing effectiveness of internal control*, Ramos states that IT controls consist of general controls and application controls. The 2006 edition of this book has been cited at least 23 times (Google, 2010c). Ramos is of the opinion that general controls are pervasive across all application systems to ensure their continued operation. He also notes that application controls relate to the accurate processing of transactions and the imbedded application controls that support this. His discussions take into account the COSO framework’s views on the internal control environment (Ramos, 2008:77, 178).

Ramos (2008:48, 77, 131) provides the following examples of general controls:

- Application systems development practices.

- Data centre operations, such as job scheduling, backup and recovery procedures.
• Logical access controls.
• Physical access security.
• System software controls, such as implementing new operating systems.

Ramos (2008:40, 131, 230) also provides the following examples of application controls:
• Matching a vendor to a pre-approved list of vendors.
• Processing of applications.
• Matching of products with purchase order files.
• Unmatched transactions posted to suspense files.
• Follow-up of unmatched transactions (manual process).

From a control objectives perspective, Ramos (2008:40, 131) argues that application controls should ensure that information remains accurate and complete, throughout processing. Only valid and properly authorised transactions should be processed. Accuracy, completeness, validity and authorisation are examples of control objectives. Notably, there are some similarities, but also differences between the views of Moeller and Ramos. Ramos provided specific examples of application controls, whereas Moeller opted for the more general classification of application controls into input, processing and output controls. As for general controls, the examples provided were not similar, giving an indication of the diverse nature of general controls.

Internal control is defined by the International Standards on Auditing (hereafter ISA) 315 (titled “Identifying and assessing the risks of material misstatement through understanding the entity and its environment”), as the processes implemented by those responsible for ensuring that the organisation’s objectives are achieved, operations are efficient and effective, and laws and regulations are complied with International Federation of Accountants (hereafter IFAC, 2009:273).

Internal controls can also be classified into the following types of internal controls, which can be viewed as characteristics of internal control (Sawyer, et al. 2003:150; Cascarino, 2007:61; The IIA, 2009:1-2):

• Preventative controls refer to controls which are designed to manage and monitor the general IT environment and are aimed at preventing a risk or event from taking place. Therefore, the control will have to be executed in advance of the risk or event.
• Detective controls refer to specific controls focusing on “acquisition, implementation, delivery and support” of IT systems, including application controls. The controls are
aimed at detecting errors or irregularities after they have taken place.

- **Corrective controls** focus on correcting the errors or irregularities after they have taken place.

The general distinction between application and general controls is evident from the discussion. The preventative and detective nature of controls are also noted. The three categories listed above are also recognised by Pickett, who adds a fourth category, directive controls. **Directive controls** aim to achieve a set objective or provide employees clear guidance (Pickett, 2010:275).

Now that auditing sources and internal controls have been considered, the attention turns to IT auditing sources, which more directly take into account IT risks.

### 4.3.5.12 Discussion of IT risk from computer auditing and IT auditing sources

IT can introduce risk into business processes, such as hampering the ability to deliver products and services effectively and efficiently (Singleton, 2009:15). Considering that IT auditors focus on technology, which supports various areas of business, it is not surprising to find IT risk being defined for computer auditing and IT auditing. This is evident from the sources referenced in this section.

In the previous section, the significance of IT risk from an internal and external audit perspective was highlighted. However, internal auditors do not always have the required skills to assess IT risk. IT auditors fill this gap, by specialising in the audit of IT controls and risks (Moran, 2005; Hinson, 2007:1). Of course, IT auditing sources could augment the knowledge of business auditors, and some books used in this section have been written for this purpose. It might also be expected that IT auditing sources expand on IT risks and controls, in contrast to internal and external audit sources. Several computer auditing and IT auditing books were reviewed in preparation for this section; however, only some of them discuss IT risk. This is not an exhaustive discussion of IT risks, but merely an overview from a number of sources.

#### 4.3.5.12.1 Views on IT risk by Davis, Schiller and Wheeler

The IT auditing book titled *IT auditing. Using controls to protect information assets*, by Davis, Schiller and Wheeler (2007:21) have identified seven areas that IT auditors should focus on:

- Entity-level controls.
• Physical facility.
• Networking and communications infrastructure.
• Operating system.
• Middleware (software facilitating communication between applications).
• Database.
• Application.

4.3.5.12.2 Views on IT risk by Bezuidenhout

In a study titled “An audit approach of the information systems auditor in an electronic commerce environment with emphasis on internet payment security”, Bezuidenhout (2002:173-174) identified a number of risks, including the corresponding control objectives, as summarised in Table 4.22.

<table>
<thead>
<tr>
<th>Control Objective(s)</th>
<th>Payment security risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorisation</td>
<td>Unauthorised changes to data / Inaccurate data.</td>
</tr>
<tr>
<td>Integrity</td>
<td>Inaccurate processing of transactions.</td>
</tr>
<tr>
<td>Privacy / Confidentiality</td>
<td>Fraudulent transactions / Interception of information.</td>
</tr>
<tr>
<td>Availability</td>
<td>Inability to identify attacks, leading to system unavailability, revenue loss and reputational damage.</td>
</tr>
<tr>
<td>Authentication / Integrity / Confidentiality</td>
<td>Repudiation of transaction.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Unauthorised access / changes to data.</td>
</tr>
</tbody>
</table>

4.3.5.12.3 Views on IT risk by Hall

In the book titled Information Technology Auditing and Assurance, Hall discusses the risks associated with a distributed data processing model, where each department has its own system, which runs the business applications (Hall, 2000:40-41):

• Inefficient use of IT resources.
• Destruction of audit trails.
• Inadequate segregation of duties.
• Programming errors.
• System failures.
• Lack of standards.
• Incompatible hardware and software.
• Difficulty in hiring competent IT specialists.
Hall also discusses risks associated with the integrity of operating systems, which should be considered from an IT risk perspective (Hall, 2000:54-55):

- Abuse of administrator access.
- Internal or external hackers exploiting security vulnerabilities.
- Viruses and other malware.

**4.3.5.12.4 Views on IT risk by Hunton, Bryant and Bagranoff**

A book by Hunton, Bryant and Bagranoff titled *Core concepts of information technology auditing*, cited at least 32 times (Google, 2010a), needs to be considered. It highlights risks which are associated with IT networks and telecommunication systems, which should be considered from an IT risk perspective (Hunton, Bryant & Bagranoff, 2004:131-136):

- Social engineering attacks.
- Physical infrastructure threats, such as fire and water, natural disasters, loss of power supply and attacks by hackers.
- Malware.
- DoS attacks.
- Weaknesses in application and security software, such as software vulnerabilities.

Hunton, *et al.* (2004:156, 157, 159, 163) also highlight the following e-business risks, which are also relevant from an IT risk perspective:

- Unauthorised logical access.
- Lack of policies related to privacy.
- Unauthorised disclosure of confidential information.
- Spyware.
- Insider and outsider (hacker) attacks.
- DoS attacks.
- Repudiation of e-business transactions.
- Loss of transaction integrity.

**4.3.5.12.5 Views on IT risk by Senft and Gallegos**

In a top-ranking IT audit book (Altius Directory, 2010) titled *Information technology control and audit*, Senft and Gallegos (2009:376) have identified several IT risks associated with application systems (presented in Table 4.23).
Table 4.23  IT risks associated with application systems (Senft & Gallegos, 2009:376)

<table>
<thead>
<tr>
<th>IT Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weak security.</td>
</tr>
<tr>
<td>Unauthorized access to data.</td>
</tr>
<tr>
<td>Unauthorized remote access.</td>
</tr>
<tr>
<td>Inaccurate information.</td>
</tr>
<tr>
<td>Erroneous or falsified data input.</td>
</tr>
<tr>
<td>Misuse by authorized end users.</td>
</tr>
<tr>
<td>Incomplete processing.</td>
</tr>
<tr>
<td>Duplicate transactions.</td>
</tr>
<tr>
<td>Untimely processing.</td>
</tr>
<tr>
<td>Communications system failure.</td>
</tr>
<tr>
<td>Inadequate training.</td>
</tr>
<tr>
<td>Inadequate support.</td>
</tr>
</tbody>
</table>

Senft and Gallegos (2009:561-565) also discuss in detail Internet-related threats, such as the potential damage that can be caused by hacker tools (scanners, password crackers and sniffers) and malware.

4.3.5.12.6  Views on IT risk by Champlain

In the book titled Practical IT auditing, Champlain (2002:A1.7) discusses threats to data security and reliability, such as fraud and mistreatment (including viruses), error and loss due to neglect, natural and manmade disasters, and the absence of IT project management practices. Champlain specifically mentions hackers as a threat to an organisation’s network (Champlain, 2002:A1.11). He also uses the general and application control classification in his discussion of mainframes and midrange systems (Champlain, 2002:A1.3, A1.6). He refers to the control objectives: existence; completeness; accuracy; validity; rights and obligations, and disclosure (Champlain, 2002:B5.5).

In another text by Champlain, he argues that the Internet is a source of significant IT risk and provides detailed discussions of the following Internet IT risks (Champlain, 2003:299-302):

- Data interception or manipulation.
- Unauthorised access.
- Hacking.
- Web-defacement.
- DoS attacks.
- Web spoofing.

4.3.5.12.7  Views on IT risk by Pathak

Pathak does not provide a discussion of IT risk, but instead focuses on IT risk objectives. In the book titled Information technology auditing. An evolving agenda, Pathak states that IT auditing determines whether an organisation’s information systems are going to achieve the following objectives (Pathak, 2005:1):
• Safeguarding of IT assets.
• Maintaining data integrity.
• Achieving organisational goals effectively.
• Efficient consumption of resources.

Pathak also discusses IT risk objectives covered during IT auditing (Pathak, 2005:5):
• Adequacy of operational controls and promoting these controls at a reasonable cost in the organisation.
• Compliance with policies, plans and procedures of organisations.
• Accounting and safeguarding of corporate information systems resources for possible loss exposure.
• Correctness and completeness of information, processed via the organisation’s information systems.
• Maintaining data integrity in information systems through internal controls.
• Effectiveness and efficiency of the organisation’s information and communication technology hardware and software.

4.3.5.12.8 Views on IT risk by Cascarino

A textbook by Cascarino, which is difficult to classify since it was written for a broad audience, including IT security, IT audit, internal and external audit, and management in general (Cascarino, 2007:xxii) needs to be considered. Cascarino is well known in the South African corporate environment for training internal auditors and IT auditors (Cascarino, 2010:5, 10). Since the textbook focuses in essence on information systems auditing, it is classified in this thesis as an IT auditing textbook. Cascarino defines IT risk in the context of the COSO ERM Framework (Cascarino, 2007:37):
• Strategic – The risk that in-house or purchased IT systems do not align with the organisation’s objectives or support its mission.
• Operations – The risk that IT systems create a burden on the organisation, resulting in poor service levels. The dependency on those systems, and the consequent unavailability of those systems, could result in operation risk.
• Reporting – The risk that the IT systems do not produce accurate, complete or timely information.
• Compliance – The risk that the IT systems could lead to breaches of laws and regulations, leading to potential losses, either financially or in reputation.
In establishing a detailed risk profile as part of a detailed risk analysis to address IT risk, Cascarino (2007:86) defines the following security-prone areas (presented in Table 4.24).

Table 4.24 Security prone areas from an IT risk perspective (Cascarino, 2007:86)

<table>
<thead>
<tr>
<th>Physical security.</th>
<th>Systems software security.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personnel security.</td>
<td>Telecommunications security.</td>
</tr>
<tr>
<td>Data security.</td>
<td>Operations security.</td>
</tr>
<tr>
<td>Applications software security.</td>
<td></td>
</tr>
</tbody>
</table>

Cascarino goes on to discuss common computer risks, including the lack of a risk evaluation, resulting in an incorrect view of computer controls. Another IT risk related to inadequate segregation of duties could be due to a lack of management’s involvement and proper allocation of responsibilities. A further IT control, inadequate access control, could be the result of poor supervision and personnel procedures. Open systems and a lack of user awareness could increase the organisation’s IT risk profile (Cascarino, 2007:77).

Cascarino also discusses the risks associated with the failure of network security, including loss of reputation, loss of confidentiality, loss of information integrity, failure of user authentication and unavailability of systems (Cascarino, 2007:322). Risks that may influence the physical or environmental security could be of a natural (for example, floods or hurricanes) or manmade nature (for example, fire or civil unrest), and the risks of this nature can be broadly divided into physical damage and destruction, theft of equipment, or loss of data confidentiality (Cascarino, 2007:330-331).

**4.3.5.12.9 Views on IT risk from a leading industry publication and journals**

A number of examples of IT risk are cited from a leading IT auditing publication and journals. A comprehensive search on Sabinet (2010) revealed only two active IT audit journals: the ISACA Journal and the “EDP audit and control and security newsletter” (hereafter EDPACS). On review, it was found that the EDPACS journal articles hold no specific view on IT risk. The “ISACA Journal” (previously titled “Information Systems Control Journal”) articles, which provide IT auditors with professional development insight (ISACA, 2007), do address IT risk from various angles. Several examples are listed here.

Firstly, the following IT risks are provided from the journal, as they relate to information security (Schlarman, 2009:27):

- “Threats to confidentiality and integrity of data.
- Threats to availability to systems.
• Management of extended enterprise.
• Management of rapidly expanding technology infrastructure.”

Secondly, the journal provides a discussion of IT risk from ISACA’s “Risk IT Framework” (Fischer, 2009a:29). It is pointed out that IT risk is defined by the IT Risk Framework as “the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise”. The categorisation of IT risk by the IT Risk Framework is also discussed (Fischer, 2009a:29):

- **IT service delivery risk** – relates to the performance and availability of IT services.
- **IT solution delivery/benefit realisation risk** – how IT projects contribute to new or improved business solutions.
- **IT benefit realisation risk** – relates to missing out on opportunities to use technology as an enabler for business processes to be more efficient and effective.

Thirdly, the journal also lists IT risks from an enterprise value inhibitor perspective, as taken from ISACA’s Risk IT Framework (Fischer, 2009c:20):

- “Unrealised or reduced business value through IT.
- Missed IT-assisted business opportunities.
- Adverse IT related events destroying value.”

Fourthly, the journal points out that IT security (which relate to IT risk) should be assessed according to the information security objectives of confidentiality, availability and integrity. This assists in the identification of related IT risks, such as unauthorised access (integrity), theft of confidential data (confidentiality) and a high reliance on IT (availability) (Singleton, 2007:21).

Lastly, a few technology specific examples which may introduce IT risk, from ISACA journals are provided, for example, wireless LAN; susceptible to IT risks of eavesdropping; unauthorised access and DoS attacks (Stanley, 2002:58-59). Another example is USB mass storage devices, which could compromise the confidentiality, integrity and availability of an organisation’s business critical information. The IT risks associated with this technology include malicious users who might use an USB to gain unauthorised access (by making use of key capturing software stored on the device). Other IT risks include storing hacker software on the devices to crack passwords or to scan a network. USB drives could also propagate viruses across a network (Tharp, 2007:28).
4.3.5.12.10 Views on IT risk from conference proceedings

Views from ISACA conference proceedings and event meetings on IT risk are also considered. It has been highlighted that IT risks need to be identified in order to ensure that an organisation achieves its business objectives. This is only possible when a clear understanding of the IT environment (including supporting infrastructure and business critical applications) has been obtained (Fried, O’Reilly & Nguyen, 2003:5).

From an information protection perspective, an organisation should monitor and remediate several IT risks, which are as follows (Greene, 2009:6-14):

- Critical business information is stored in an unsafe location (also referred to as rogue data), where it can be obtained by an unauthorised individual.
- Weak logical access controls implemented to protect vital information.
- Erroneous and wrongly configure perimeter devices, such as firewalls.
- Failure to encrypt business critical information, when stored or in transit.
- Unauthorised access to business critical data stored on an employee’s home computer (when working from home).
- Website and application vulnerabilities, allowing unauthorised access to business critical information.
- Malicious network activity, such as hacking attacks, malicious insider activity and third party errors.
- Lack of user awareness, making employees vulnerable to social engineering attacks.
- Lack of information security governance, to ensure information is protected pervasively across the organisation.

4.3.5.12.11 Views on controls from IT auditing sources

All of the IT risks presented could be avoided or mitigated by some form of control (Young, 2006:21). Cascarino defines a control as follows (Cascarino, 2007:57):

Any action taken by management to enhance the likelihood that established objectives and goals will be achieved.

Controls are designed to achieve certain control objectives. Control objectives assist management in ensuring that controls are designed to achieve the intended objectives (Cascarino, 2007:61). Cascarino (2007:10, 268) has identified the following control objectives: confidentiality, integrity, availability, accuracy, completeness, validity and
Auditors (including IT auditors) need to identify control objectives to assess whether controls achieve the required “result or purpose” (Petterson, 2005:41). The discussions on IT risks are often mixed with references to control objectives. Parker (2006:5.05) has defined the following control objectives: confidentiality, processing integrity, availability, security and online privacy. It is submitted that controls achieve the opposite of what risks will achieve. Repeatedly, in the discussion of IT risk, the characteristics used to describe IT risks are the exact opposite of control objectives, for example unauthorised transactions vs. authorised transactions. Therefore, when considering IT risk, the identification of the applicable control objectives will assist management in the appropriate design of internal controls, which will consequently adequately address the IT risk. Cascarino concurs with views on internal control in section 4.3.5.11: internal controls can be classified as corrective, detective or preventative in nature (Cascarino, 2007:61).

Lastly, an ISACA Journal article on the discussion of general and application controls is considered (Sayana, 2002:16-18). Sayana sees general controls as the controls surrounding the information systems. This may include both organisational and administrative controls, policies and procedures, staff training and staff availability. Further aspects to be considered are infrastructure and environmental controls, and physical access controls. Application controls relate to the applications which process business transactions. Controls should be imbedded, which ensures that business rules are followed, accuracy of processing is achieved, and only valid data input is allowed. Sayana classifies logical access controls under application controls, in contrast with the views of Ramos (2008:131) and the IIA’s GTAG 8 (Bellino & Hunt, 2007:2), which classifies it under general controls.

Again, the classification of controls into general and application is recognised. The preventative and detective nature of controls are also noted.

4.3.5.13 Discussion of IT risk from SAICA standards

The focus in this section is on SAICA auditing standards. Over the years SAICA has released a number of standards on IT and IT-related risks, creating awareness among its members on how to deal with IT risk. Even though, over time, many of the standards have been replaced, some of the publications that have been withdrawn still provide valuable insights into IT risk, and, therefore, some of these publications will be discussed below.
4.3.5.13.1 Views on IT risk from SAICA’s South African Auditing Standards

The first auditing guideline published by SAICA that related to IT, titled “Auditing in a computer environment”, later to be replaced by South African Auditing Standard (hereafter SAAS) 401, highlighted the following risks associated with computerised systems (SAICA, 1989:22, 32, 74):

- Continued processing of errors due to flawed logic.
- Accidental or intentional changes to data and programs.
- The absence of a paper trail, which complicates the investigation of errors.
- Automated data processing, without any physical evidence.
- Lack of physical reports.
- Concerns related to systems development, physical access and operations of the computer function.

Another auditing standard that is relevant in providing an overview of IT risk is “Auditing in a computer information systems environment” (SAAS 401), which recognises that IT could have a significant impact on the way transactions are generated, processed, stored and communicated. Some of the key IT risks that are relevant to the internal control environment include a lack of transaction trails, which complicates the process of identifying errors and irregularities. Further, the automation of traditional business processes leads to the loss of segregation of duties, which increases the likelihood of accidental initiation of financial transactions, which is also mentioned. Programming errors made during the development of the business applications could lead to the erroneous processing of transactions. Other risks which have implications for the general controls environment of IT, include poor program development and maintenance, lack of physical access and logical access controls (SAICA, 2002:SAAS 401.01, .03, .09, .11).

The auditing standard “Risk assessment and internal control – Computer information systems characteristics and considerations” (SAAS 4011) argues that IT has produced several new risks that are unique to the IT environment. For example, IT personnel might be familiar with the internal control weaknesses that exist in the applications, increasing the likelihood of program or data alteration. The centralisation of programs and data also increases the risk of unauthorised access and alteration of programs and data. Automation of once-manual business processes could lead to data entry without supporting documents, a lack of a visible transaction trail and less visible output, which increases an organisation’s operational risk. Other IT risks introduced by automation include consistent erroneous
processing of transactions, and unauthorised, incorrect or incomplete input of transactions and data. Furthermore, single-entry multi-update controls could cause multiple erroneous entries in financial accounts, while storage of huge volumes of data on transportable storage devices increases the risk of theft or destruction (SAICA, 2002:SAAS 4011.01-.04).

4.3.5.13.2 Views on IT risk from SAICA Practice Statements

SAICA practice statement “IT environments – standalone personal computers” (SAAPS 1001) points out that fewer physical security measures or general controls might be in place to protect standalone PCs. This could lead to the theft of PCs or storage media. Access control might be weak, and users might install unauthorised software, which could introduce viruses. Less rigour might be applied to a standalone PC, to ensure that software is up to date to avoid processing errors (SAICA, 2002:SAAPS 1001.01, .06, .08, .09, .10, .11, .13).

SAICA practice statement “IT environments – on-line computer systems” (SAAPS 1002) states that IT risk has increased through the lack of a clear transaction trail supporting on-line data entry and the possible access by unauthorised users. The risk of unauthorised access is aggravated by access from a remote site, in particular where authentication controls are lacking. Advancements in business applications allow users to perform multiple functions not previously available in older systems. However, this also increases the risk of having access to sensitive application functions, which could be used to alter or delete data (SAICA, 2002:SAAPS 1002.01, .15, .17, .25).

SAICA practice statement “IT environments – database systems” (SAAPS 1003) discusses the key concern of the integrity, security and completeness of data. IT risks can emerge from the absence of application program standards, since databases have to integrate closely with the business applications. Issues may arise related to data ownership, which impacts decisions of who may access the database and ensuring that adequate segregation of duties are in place to prevent access to sensitive data. Database technology increases the risk of IT, in that it requires specialised management, which increases an organisation’s human resource risk (SAICA, 2002:SAAPS 1003.18, .21, .24, .26).

SAICA practice statement “Electronic commerce – effect on the audit of financial statements” (SAAPS 1012) discusses several IT risks associated with this technology that increase the organisation’s business risk. The loss of transaction integrity, aggravated by the lack of an audit trail, is of key concern. E-commerce systems facilitate communication between transacting organisations, which by implication increases the risk of unauthorised access.
Huge reliance is placed on these systems, and the failure of the supporting IT infrastructure could lead to reputational risk for the company. The compliance risk of the organisation is also at risk, due to issues with transactions made across international borders and complying with legislation of other countries (SAICA, 2003:706-707).

**4.3.5.13.3 Conclusion on IT risk from SAAS and SAAPS statements**

Although the SAAS and SAAPS statements each cover a different topic, they all highlight very similar IT risks. The focus of these standards is on the internal control environment and the automation of what was traditionally always manual business processes. As a result, a number of key IT risks have been highlighted from a general controls perspective (as defined in section 4.3.5.11), such as a lack of segregation of duties and the lack of physical access control to prevent theft of IT equipment and removable media. There is also a focus on application-specific IT risks (as they relate to application controls, also defined in section 4.3.5.11), such as unauthorised access, which may lead to the alteration of programs and data, and risks associated with the input, processing and output of business transactions.

**4.3.5.13.4 Views on IT risk from International Standards on Auditing and International Auditing Practice Statements**

On 1 January 2005, the Auditing and Assurance Standards Board (hereafter AASB) of the then Public Accountants’ and Auditors’ Board (hereafter PAAB) decided to replace the SAAS and SAAPS standards with the ISAs and the International Auditing Practice Statements (hereafter IAPS) issued by the International Auditing and Assurance Standards Board (hereafter IAASB) of the IFAC. This decision was based on the fact that South African standards have always been based on the international standards (Independent Regulatory Board for Auditors (hereafter IRBA, 2009:1, 2). However, the IAASB “concluded that the need for certain IT-related practice statements has been superseded by the assumption of computer processing in its revised standards on understanding the business and assessing the risks of misstatement”. Consequently, IAPS 1001, 1002, 1003 and 1009 were withdrawn effective 31 December 2004 (McGladrey & Pullen LLP, 2005:3).

Cognisance must also be taken of two existing SAICA standards which specifically include references to IT risk. In ISA 315 “Understanding the entity and its environment and assessing the risks of material misstatement”, the impact of IT on the elements of internal control is discussed. The standard lists the following IT risks which could potentially affect an organisation’s internal controls (SAICA, 2007:ISA 315.13):
• Placing reliance on systems which process data inaccurately or process inaccurate data, or both.
• Unauthorised access to data, leading to changes or deletion.
• Recording of fictitious transactions.
• A lack of segregation of duties.
• Obtaining access privileges beyond those of your job description.
• Unauthorised changes to data, systems or programmes.
• Inability to access data (DoS).

In ISA 402 “Audit Considerations Relating to Entities Using a Service Organization” consideration is given to computer systems service organisations and the accountability they take for ensuring accuracy, security and completeness of the organisation’s transactions, records and data. The IT procedures and controls around journals and accounting records are of particular interest here (IFAC, 2010:ISA 402.3). Inadequate IT system resources could lead to the risk of material misstatement (IFAC, 2010:ISA 402.A24).

Given the prominence of issues related to electronic commerce in this thesis, the associated risks as expounded by SAICA’s IAPS 1013 “Electronic Commerce – Effect on the audit of financial statements” are relevant. These include (SAICA, 2007:IAPS 1013.5, .6):
• Loss of transaction integrity.
• Virus attacks and e-commerce fraud through unauthorised access.
• System failures, which lead to loss of data.
• Not complying with relevant legal and regulatory requirements, in particular, international cross-border transactions.

4.3.5.13.5 Conclusion on IT risk from ISA and IAPS standards

On the whole, the IT risks highlighted by the SAICA ISA and IAPS standards are very similar to older SAAS and SAAPS standards. There are a few unique risks highlighted by the SAICA ISA and IAPS standards which reflect new prevailing IT risks in today’s complex IT environments. ISA 315 highlights the IT risk DoS. Naturally, situations did exist in the past where valid users could not access their business applications. However, today, DoS could cripple a significant portion of an organisation’s operations. IAPS 1013 highlights the IT risk “virus attacks”, which, again, is a significant risk for most organisations connected to the Internet. In today’s corporate environment, viruses can very easily be delivered via e-mail and most likely have to be managed as daily events, as opposed to a risk that may only
occur in the future. In the past, not all organisations made use of e-mail, and hence this particular risk may have been less of a concern. Therefore, one can conclude that the introduction of new technologies brings along with it new IT risks and consequently the latest audit standards have to stay abreast of the impact of new IT risks.

4.3.5.14 Discussion of IT risk from IIA publications

The significance of IT risk from an internal audit perspective has been established in section 4.3.5.10. The IIA is the leading professional body for the internal audit profession and hence its reflection on IT risk needs to be considered in this thesis (The IIA, 2010d).

4.3.5.14.1 Views on IT risk from IIA’s Practice Advisories

The IIA has issued a number of Practice Advisories (hereafter PAs), to assist the internal audit community in discharging its responsibilities. Only two of these are applicable from an IT risk perspective:

- **Control and Audit Implications of E-commerce Activities** (PA 2100-6) highlights several security threats or IT risks associated with e-commerce solutions, such as physical attacks, viruses, DoS, identify theft, unauthorised access to data and unauthorised disclosure of data. The guidance document argues that maintaining transaction integrity is complicated by the complex interaction of e-commerce solutions with other systems and companies. Compliance issues, such as tax jurisdiction, data privacy, legality of contracts outside country of origin and accounting issues, all pose a risk. The possibility of fraud is significantly higher in an e-commerce environment, with unauthorised movements of funds and duplicate payments a definite reality. Various risks can result from hacking attacks, such as destruction of data or interception of transactions (The IIA, 2010b:1-2).

- **Application Systems Review** (PA 2100-9) highlights application risks which could lead to unauthorised access, system unavailability and loss of data integrity. The non-availability of applications to support normal business operations adds potential IT risks faced by an organisation. IT risks associated with the confidentiality and privacy of data are also of concern (The IIA, 2010b:1-4).

It should be noted that the IIA withdrew the PA 2100 series. IT issues and risks are now addressed as part of the GTAGs (The IIA, 2010a).
4.3.5.14.2 Views on IT risk from IIA’s Global Technology Audit Guides

The IT risks highlighted by the IIA are, in general, similar to the IT risks defined by SAICA. The IIA’s Practice Guides (hereafter PGs) GTAG has been published with the intention of sensitising audit executives on key technology issues from an audit perspective (The IIA, 2010c). It provides insight into the IT risks most significant from the IIA’s and consequently from an internal audit perspective. Only relevant GTAGs, with a focus on IT risks, are listed here:

- *Information Technology Controls* (GTAG 1) does not provide a comprehensive discussion of IT risk; however, IT controls are defined to address IT risks and are therefore relevant for the purposes of this discussion (The IIA, 2005:iv, 5-8):
  - Policies – In the absence of well-defined policies, employees might operate outside of their prescribed mandates, neglecting, for example, their security and privacy responsibilities. Business users might neglect their data ownership responsibilities.
  - Standards – In the absence of detailed standards, for example, systems may be inadequately configured, introducing IT vulnerabilities which could be exploited by hackers. Systems that contain control weaknesses may be developed, which could lead to processing errors.
  - Organization and Management – Ill-defined separation of duties may lead to users having access to incompatible functions. The lack of financial controls could lead to the risk of significant overspend on IT development projects. The lack of change management processes may lead to unauthorised changes to production systems, which could introduce fraud.
  - Physical and environmental controls – The lack of physical controls could lead to damage or theft of IT equipment. The lack of environmental controls, such as a fire suppression system, could lead to significant damage to equipment in the event of a fire.
  - System software controls – This category refers to software which supports business applications, such as operating systems, database and network software. An example of an IT risk is the poor configuration of operating systems, which could lead to security breaches.
  - Systems development controls – Applications may be developed without adequately consulting the end-user, or following a process of detailed system design, to ensure all requirements are incorporated. This may lead to the absence of critical controls, which could lead to error or fraud once put into production.
Application-based controls – The basic building blocks of applications are input, processing, output and audit trail functionality. The absence of input controls may lead to data integrity issues. The absence of processing controls may lead to incomplete, inaccurate or unauthorised processing of business transactions. The absence of output controls might lead to unauthorised disclosure of sensitive information. The absence of an audit trail would make it difficult to investigate errors and fraud.

- **Change and Patch Management Controls: Critical for Organizational Success** (GTAG 2) states that a lack of change management could lead to business disruptions or unauthorised changes. To derive the maximum business benefit, the risks that should be avoided include failing to complete the requested change within time, or budget, or by not meeting the expected business requirements (Taylor, Allen, Hyatt & Kim, 2005:38). A lack of change and patch management control might introduce IT risks which could for example introduce malicious code into the production environment, which either allows fraudulent activity or introduces vulnerabilities, exploitable by hackers.

- **Management of IT Auditing** (GTAG 4) provides a broad framework for establishing and managing an IT audit function, including the scope of IT auditing. The guide recognises that there are two types of IT risks: pervasive and specific. Pervasive risks are risks that may affect the organisation as a whole. A specific risk will have more of a direct impact on a process or system. IT risks originate from the issues related to the availability, security, integrity, confidentiality, effectiveness or efficiency of IT systems and operations (Juergens, Maberry, Ringle & Fisher, 2006:7).

- **Managing and Auditing Privacy Risks** (GTAG 5) states that customers are concerned about the way organisations protect their personal information. There is a real risk of identity theft, and management has to find ways of managing it appropriately (Hahn, Askelson & Stiles, 2006:3, 4, 9).

- **Managing and Auditing IT Vulnerabilities** (GTAG 6) points out that IT vulnerabilities leave an organisation exposed to hackers and malware such as viruses, and worms. An effective strategy geared towards the identification, remediation and improvement of IT vulnerabilities is required (Romanosky, Kim & Kravchenko, 2006:1, 4-6). This GTAG has particular applicability in the context of this study, since the use of ethical hacking will be explored as an effective response to hacking.

- **Information Technology Outsourcing** (GTAG 7) has identified the risks that should be managed as part of the IT outsourcing arrangement: information protection, network security, physical security, personnel security and logical access controls to
Applications (Ray, Ramaswamy & Ganguli, 2007:1, 15-16). Outsourcing IT might have significant cost benefits for organisations; however, it could also introduce IT risks, such as unauthorised access or exposure to malicious software.

- **Auditing Application Controls** (GTAG 8) indicates how applications can present numerous risks, due to a lack of input, processing or output controls. When applications are upgraded or replaced, previously defined controls might be left out, exposing the organisation to risk. Unauthorised or invalid access to applications is a common risk (Bellino & Hunt, 2007:5, 9). Web application vulnerabilities are often exploited by hackers today. Web developers must build in similar controls into web applications, compared to their standalone counterparts. Bellino and Hunt (2007:2) also note that IT controls can be divided into application controls and general controls. Application controls refer to the controls built into applications, which focus predominantly on input, processing, output and integrity controls, and management trail. Application controls ensure that the completeness, accuracy and validity of transactions and data are achieved. General computer controls refer to controls within the general IT environment, which will support application controls. General controls include logical and physical access controls, system development life cycle (hereafter SDLC), change management, backup and recovery controls, and computer operation controls (Bellino & Hunt, 2007:2).

- **Identity and Access Management** (GTAG 9) points out that identity and access management controls improve the risks associated with access to systems, how the access is managed and to which job profile it is linked (Rai, Bresz, Renshaw, Rozek & White, 2007:1, 2). The insider threat, as discussed in 3.5.3.6, closely linked with hacker activity, could be exacerbated by poorly managed access controls.

- **Business Continuity Management** (GTAG 10) enables an organisation to continue operations after a significant incident (Everest, Garber, Keating & Peterson, 2008:3). In the context of this study, it is important to note that a hacking incident could cause severe business disruption, calling into action the BCP plan.

- **Developing the IT Audit Plan** (GTAG 11) indicates that independent IT risk assessments should be performed, in particular on new technologies which may impact the organisation (Rehage, Hunt & Nikitin, 2008:1).

- **Auditing IT Projects** (GTAG 12) highlights that IT projects are often at risk of failing, which might severely affect an organisation (Wegrzynowicz & Stein, 2009:3).

- **Fraud Prevention and Detection in an Automated World** (GTAG 13) indicates that there are several IT fraud risks, such as insufficient physical controls, access to systems or data, changes to system programs or data, fraudulent activity by
independent contractors, conflict of interest with suppliers or third parties, copyright infringement and misappropriation of company data by third parties (Askelson, Lanza, Millar, Prosch & Sparks, 2009:3-5).

- Auditing User-developed Applications (GTAG 14) highlights several risks associated with user-developed applications (for example spreadsheets), lack of development practices and version control, data download issues, increased complexity, lack of documentation and support, limited input and output controls and lack of formal testing (Bellino, Ochab & Rowland, 2010:2-3).

- Information Security Governance (GTAG 15) points out that the board requires information security, to ensure confidentiality, integrity and availability risks are mitigated and reported (Love, Reinhard, Schwab & Spafford, 2010:3). The information security governance aspect will be further explored in chapter 5.

4.3.5.14.3 Views from Guide to the Assessment of IT Risk

Another key piece of guidance published by the IIA is the “Guide to the Assessment of IT Risk (GAIT) for Business and IT risk” (referred to as GAIT-R). Despite the title of the guide, it does not discuss IT risk in detail. Instead, it provides guidance on how key controls can be identified, to ensure business goals and objectives are achieved. It generally considers IT risk from a business perspective (and even labels IT risks as business risks) (The IIA, 2008:6). The GAIT-R is built around four principles. These are (The IIA, 2008:2):

- “Principle 1: The failure of technology is only a risk that needs to be assessed, managed, and audited if it represents a risk to the business.
- Principle 2: Key controls should be identified as the result of a top-down assessment of business risks, risk tolerance, and the controls - including automated controls and IT general controls (ITGCs) - required to manage or mitigate business risk.
- Principle 3: Business risks are mitigated by a combination of manual and automated key controls. To assess the system of internal control to manage or mitigate business risks, key automated controls need to be assessed.
- Principle 4: ITGCs may be relied upon to provide assurance of the continued and proper operation of automated key controls.”

As part of principle 4, the guide provides the following examples of general controls, towards the achievement of IT control objectives (The IIA, 2008:9):

- Applications should be tested before being migrated into production.
- Data should be protected against unauthorised modification.
Problems or incidents encountered during operations should be reported, analysed and corrected.

4.3.5.14.4 Conclusion on IT risk from IIA publications

The IIA has provided comprehensive guidance on IT risk and control, although notably mostly from an auditing perspective. Similar to other sources on IT risk, application controls are also divided into the general classification of input, processing and output controls. A clear distinction is also made between general and application controls. Overall, there is recognition of the significance of IT risk in business and the fundamental need for internal control as a response (further discussed in chapter 5).

4.3.5.15 Discussion of IT risk from ISACA sources

ISACA, a leading global IT governance and IT audit professional body (ISACA, 2010a), has issued a number of auditing guidelines applicable to the IT environment. Particularly in the context of this thesis, IT risk from ISACA’s perspective is significant. ISACA’s standard, *Use of Risk Assessment in Audit Planning* (S11) encourages IT auditors to use risk assessments as a means of understanding the risk landscape and preparing the audit plan accordingly (ISACA, 2010c:S11.03). Even though the risks identified by ISACA are wide-ranging, risks have also been narrowly identified for specific technologies.

4.3.5.15.1 Views on IT risk from ISACAs Guidelines

ISACA has published several guidelines that provide advice on how to audit various technologies. The risks discussed in these guidelines are highlighted below:

- **Application Systems Review** (G14) highlights application risks which could lead to system unavailability, loss of data integrity, or breach of security due to unauthorised access (ISACA, 2010c:G14.2.1.3).

- **Effect of Third Parties on an Organisation’s IT Controls** (G16) indicates how weaknesses in third-party systems could lead to unauthorised access and changes to systems or data, which could make the systems unavailable (ISACA, 2010c:G16.5.1.2).

- **Enterprise Resource Planning (ERP) Systems Review** (G21) makes the case that the integrated nature of ERP systems increases the IT risk in an organisation, specifically related to, for example, application security, data conversion and integrity, and
business continuity (ISACA, 2010c:G21.2.2.1). The inherent complexities of new integrated applications increase an organisation’s IT risk. It is therefore important for management to understand the nature of the systems they install and what risks they inevitably introduce.

- **Business-to-consumer (B2C) E-commerce Review (G22)** notes the far-reaching effect of e-commerce applications on business. It recognises the risks, such as viruses, associated with the Internet, which is used as a primary communication medium to facilitate e-commerce transactions. Another key risk is the integrity of data during transmission, including the authenticity of the source. Privacy of customer details, regulatory implications, authorisation of payments, disaster recovery and third-party confidentiality agreements are all key concerns here (ISACA, 2010c:G22.2.3).

- Several IT security risks are associated with **Internet Banking (G24)**. These include authentication of customers, non-repudiation of transactions, segregation of duties, lack of authorisation controls, internal and external fraud, confidentiality and integrity of data, the existence of audit trails and security risks associated with third parties (ISACA, 2010c:G24.6.1.3). When working with confidential client data, the banking sector will have to give due consideration to these IT risks.

- **Review of Virtual Private Networks (G25)** highlights a number of security risks associated with IT, including failure to clearly assess the IT security risks associated with VPNs and the lack of a security program to mitigate risks associated with information assets linked to VPNs. In addition, data exposure could exist when entering or leaving the VPN, and failure to encrypt unprotected data when traversing across internal and external networks is another area of concern (ISACA, 2010c:G25.3.2.1). VPN technology enables secure communication channels. Yet, when not configured securely, it could increase the IT risk of an organisation (own deduction).

- **Mobile Computing (G27)** devices significantly increase the business risk profile, due to their portability. The theft or loss of data is a definite concern. Mobile devices could also transfer viruses or worms to the organisation’s network. Unauthorised access to data stored on mobile devices is another concern, due to the simple nature of the operating systems used on mobile devices (ISACA, 2010c:G27.4.2.2). Confidentiality and data privacy are not confined to the walls of the organisation anymore. New technologies also expose organisations to new IT risks (Rehage, *et al.* 2008:1). Management will have to devise appropriate responses on how to deal with these new emerging risks.

- **General Considerations on the Use of the Internet (G33)** lists several threats
associated with linking a corporate network to the Internet. Three groups of attacks are distinguished. Firstly, passive attacks include monitoring networks for username and password combinations, tapping confidential data, or deploying spyware to intercept client details. Secondly, active attacks include targeting security weaknesses, obtaining passwords via software tools, masking a PC with a legitimate and trusted network address in order to elicit information, making use of viruses, Trojans or worms to cause damage and disruption, and exploiting misconfigured IT systems. Thirdly, service attacks include DoS attacks or rerouting legitimate transactions to a false website (ISACA, 2010c:G33.2.2).

In brief, ISACA's professional guidelines cover a number of IT-related technologies that are typically found in the business world. Similar to the IIA's GTAG series, the guidelines place significant focus on the risks posed by cybercrime-related threats. There is also a lot of focus on unauthorised logical access, which is a fundamental IT risk that can be mitigated by basic logical access controls.

4.3.5.15.2 Views on IT risk from ISACA's The Risk IT Framework

Another important document published by ISACA to be considered here is “The Risk IT Framework”. The document is aimed at assisting organisations in the management of IT risks. The document also states, “IT risk is the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise”. The focus is therefore on aligning IT risk management practices with overall IT governance and IT process management (ISACA, 2009:7). The framework sees IT risk as a pervasive risk across an organisation, as depicted in Figure 4.5. The framework does not define or list detailed IT risks. Instead, it provides guidance, processes and metrics to manage IT risk.

Figure 4.5 Positioning IT risk in the organisation (adapted from ISACA, 2009:11)
The framework divides IT risk into three categories (ISACA, 2009:11):

- **IT service delivery risk**: Relates to the performance and availability of IT services, which could decrease an organisation’s value.
- **IT solution delivery/benefit realisation risk**: Relates to the contribution of new IT solutions towards improving the organisation’s business processes, typically accomplished via IT development projects.
- **IT benefit realisation risk**: Relates to opportunities to improve the effectiveness of existing business processes and seek new business initiatives.

The framework assists management in the identification of risk and making the appropriate decisions in terms of accepting risk versus reward. The essence of this framework is encapsulated in the following quote (ISACA, 2009:11):

> Without a clear understanding of IT risk, senior executives have no frame of reference for prioritising and managing enterprise risk.

### 4.3.5.15.3 Conclusion on IT risk from ISACA statements

Similar to the guidance provided by the IIA, ISACA has provided guidance on IT risk and control, covering a broad range of issues and technologies found in the business world. The focus is predominantly on the recommendation of controls that could be used to address the applicable IT risks. ISACA also provides guidance on how to manage IT risk and has provided frameworks, such as the Risk IT Framework, to do so. ISACA is of course well known for its collaboration with the ITGI, discussed next.

### 4.3.5.16 A perspective on IT risk from IT Governance Institute publications

The ITGI has as its purpose to assist business leaders in aligning IT with business and has developed several guidelines to assist business leaders with their IT governance responsibilities. The literature suggests that the ITGI emphasises the significance of IT risk within an organisation and provides overall guidance to executive management towards effective management thereof (ITGI, 2010a).

#### 4.3.5.16.1 Views on IT risk from ITGI’s CobiT

The ITGI is closely aligned with ISACA. They are mutually responsible for the development and publishing of CobiT. CobiT is a widely used best practice framework for IT governance,
CobiT provides an effective IT Governance Framework that focuses on aligning IT with all aspects of business (ITGI, 2010b:5-6). CobiT focuses on five IT governance focus areas: strategic alignment, value delivery, resource management, risk management and performance measurement (ITGI, 2010b:6). As regards the focus of risk management, CobiT states that a risk awareness is required “by senior corporate officers, a clear understanding of the enterprise’s appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise and embedding of risk management responsibilities into the organisation” (ITGI, 2010b:6).

In order to satisfy business objectives, CobiT (ITGI, 2010b:10-11) has defined the following information criteria, which are very similar to control objectives: confidentiality, integrity, availability, effectiveness, efficiency, compliance and reliability. CobiT also distinguishes between IT general controls and application controls. IT general controls include controls that are entrenched in IT processes and services. Controls entrenched in business applications are referred to as application controls, and are aimed at achieving completeness, accuracy, validity, authorisation and segregation of duties (ITGI, 2007a:15).

### 4.3.5.16.2 Other views on IT risk from ITGI guidance documents

ITGI has published numerous white papers, surveys and guidance documents. These assist industry leaders in performing their IT governance duties (ITGI, 2010c). Several ITGI guidance documents have been reviewed for this section; however, only a few of them cover IT risk.

Firstly, a document published by the ITGI that is of particular importance from an IT risk perspective is the “CobiT Security Baseline Information Security Survival Kit”. The document identified that gaps in security are usually caused by (ITGI, 2007c:12):

- Weaknesses in the risk and threat management process.
- New vulnerabilities introduced by new technologies.
• Failure to patch systems timeously.
• Increase in networking and mobile computing.
• General lack of security attentiveness.
• Lack of discipline in applying appropriate controls.
• Increased sophistication of hacker, fraudster, criminal and terrorist attacks.
• Changing legislative, legal and regulatory security requirements.

Secondly, in the document titled “IT Governance Global Status Report – 2008”, a number of IT risks that are top of mind for executives globally are highlighted (ITGI, 2008d:45):

• Inadequate number of staff.
• IT service delivery issues.
• Significant investment in IT with no tangible return.
• Poor IT development practices.
• Lack of competent staff.
• Issues with vendors and third-parties.
• Lack of knowledge management ability.
• Misalignment between IT and business strategy.
• Lack of effective electronic storage.
• Poor DRP and BCP.
• Inability to meet compliance requirements.
• Security and privacy incidents.

Thirdly, a document titled “Unlocking Value: An Executive Primer on the Critical Role of IT Governance” alludes to the pervasiveness of IT risks. The document emphasises that IT risks need to be managed to ensure they do not affect the organisation’s ability to operate competitively in a demanding economy (ITGI, 2008e:9).

Fourthly, in the document titled “Information Risks: Whose Business Are They?”, the ITGI argues that there is no generic IT risk definition, but goes on to define a set of related IT risks (ITGI, 2005b:9):

• “Investment or expense risk: The risk that the investment being made in IT fails to provide value for money or is otherwise excessive or wasted. This includes consideration of the overall portfolio of IT investments.
• Access or security risk: The risk that confidential or otherwise sensitive information may be divulged or made available to those without appropriate authority. An aspect of this risk is privacy, the protection of personal data and information, which in many
countries and regions is required by law to be addressed.

- **Integrity risk**: The risk that data cannot be relied on because the data is unauthorised, incomplete or inaccurate.
- **Relevance risk**: The risk associated with not getting the right information to the right persons (or process or systems) at the right time to allow the right action to be taken.
- **Availability risk**: The risk of loss of service.
- **Infrastructure risk**: The risk that an organisation does not have an information technology infrastructure and systems that can effectively support the current and future needs of the business in an efficient, cost-effective and well-controlled fashion (includes hardware, networks, software, people and processes).
- **Project ownership risk**: The risk of IT projects failing to meet objectives through lack of accountability and commitment.”

Fifthly, the document titled “Information Security Governance: Guidance for Information Security Managers” encourages the use of CobiT’s maturity levels. In particular, the organisation’s IT risk management processes can be assessed with the maturity levels. For example, the IT risk management process will be rated as “2 Repeatable but intuitive”, when the organisation understands IT risks and has developed some approach towards managing IT risks (although not fully mature yet) (ITGI, 2008c:61).

### 4.3.5.16.3 Conclusion on IT risk for the ITGI

The guidance provided by the ITGI on IT risk is predominantly from an IT governance perspective. One of its most widely used frameworks, CobiT, provides comprehensive guidance on IT controls, rather than IT risk itself. Similar to other sources referenced in this chapter, CobiT also distinguishes between general and application controls. Most of the IT risks identified in the ITGI’s guidance documents should be of key consideration to the board of directors, since the IT risks could negatively affect the business strategy. This illustrates the significance of responding to IT risk towards achievement of business objectives.

### 4.3.5.17 Conclusion

Technology risk is a collective term that includes all manner of technological advances, ranging from operational to pure IT areas. There are many factors that affect technology risk, ranging from technology obsolescence to the complexity of implementing it within an organisation.
The literature study has shown that new technology could increase an organisation’s technology risk due to the unavailability of skills to support it. New technology may introduce new vulnerabilities, due to the modification or misconfiguration of functionality. High-volume processing facilitated via new high-speed technologies could replicate errors. Failure to identify unknown risks associated with new technology could also increase technology risk. With the continued advancement in technology, organisations will have to deal with associated uncertainty and risks introduced by new technology. On the other hand, outdated technology could also increase technology risk. Outdated technology could stunt the growth of an organisation, increase the likelihood of system failure and create a business continuity scenario or lead to costly maintenance and support.

The literature reviewed in this section indicated that IT risk could be viewed as a sub-component of technology risk. Systems risk can be viewed as synonymous with IT risk, and is often discussed in the same context. The three concepts (IT, system and technology risk) are related to each other and sometimes even used interchangeably. As regards IT risk, this aspect of technology risk carries a lot of weight within King II and King III. King II places emphasis on the impact of IT on business and technology and highlights the fundamental changes brought on by technology, such as e-business initiatives. The threats introduced by technology are also highlighted. King III takes an even more focused stance on IT risk, and highlights the achievement of successful IT governance through appropriate frameworks and risk management processes. The significance of IT is embodied in the seven principles defined by King III for the governance of IT.

There are countless granular risks associated with IT, pervasively affecting many parts of an organisation’s business, interlinking with the organisation’s business risks. It is not possible to formulate one definitive definition for IT risk. Rather a broad range of views can be advanced. IT risk contains within it elements which could lead to failure or misuse, resulting in the unavailability of IT. IT risk might also threaten the achievement of business objectives, due to weaknesses in information systems, internal controls and supporting processes.

Reflecting on the overview of the definition and scope of IT risk presented above, it is clear that internal and external audit, IT audit, IT risk and information security management and professional association publications hold a range of views on the matters. But a careful analysis of the literature presented reveals a trend, in that the IT risks listed in Table 4.25 are common to many of the sources and granular IT risks presented, and point to common IT risk themes that present a picture of the scope of IT risk that should be addressed at different levels for corporate governance purposes. It is not intended to be an exhaustive list,
but rather a reflection on the most commonly recurring IT risk themes. This list of common IT risk themes will be used in the remainder of this chapter to facilitate the discussion of the links between IT risk, business risks and hacking.

A second component to consider is the classification of IT risks into general and application controls, something that has been suggested by many authors reviewed in this chapter. General controls relate to the controls supporting the IT environment, and include aspects such as physical access and disaster recovery. Application controls relate to the input, processing and output controls of application systems. Given the numerous examples of general and application controls provided in this section and the common definition of general and application controls provided, it is possible to apply this classification to the common IT risk themes listed in Table 4.25. This is done by grouping the IT risks, which affect the general supporting environment of application systems, under general controls. Similarly, those risks that affect application system controls specifically can be grouped under application controls, with further sub-groupings. Therefore, for application controls, rather than referring to the specific application control detail, reference will be made to the application grouping, unless specific examples are provided.

**Table 4.25  Common IT risk themes (own summary)**

<table>
<thead>
<tr>
<th>General controls:</th>
<th>Application controls:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Unauthorised physical access / lack of physical access control and security.</td>
<td>• Unauthorised transactions / lack of input documentation.</td>
</tr>
<tr>
<td>• Lack of compliance with IT policies and procedures, legal and regulatory requirements.</td>
<td>• Incomplete, inaccurate or unauthorised processing of transactions and data / application errors.</td>
</tr>
<tr>
<td>• Business and IT disruption.</td>
<td>• Lack of output documentation.</td>
</tr>
<tr>
<td>• Inadequate IT operations and support.</td>
<td>• Unauthorised changes to data, systems and programmes.</td>
</tr>
<tr>
<td>• Theft or damage to IT equipment.</td>
<td>• Theft, loss or damage to data and programmes.</td>
</tr>
<tr>
<td>• Inadequate change / project management practices.</td>
<td>• Incorrect (integrity), untimely and incomplete information and data.</td>
</tr>
<tr>
<td>• Misuse of IT / irregularities and fraud.</td>
<td></td>
</tr>
<tr>
<td>• Cybercrime.</td>
<td>• Communications failure / interception of data during transmission.</td>
</tr>
<tr>
<td>• Unauthorised logical access.</td>
<td>• Problematic system interfaces.</td>
</tr>
<tr>
<td>• Inadequate IT performance.</td>
<td></td>
</tr>
<tr>
<td>• Complexity of IT.</td>
<td></td>
</tr>
<tr>
<td>• Inefficient use of IT resources.</td>
<td></td>
</tr>
<tr>
<td>• IT human resource deficiencies.</td>
<td></td>
</tr>
</tbody>
</table>
• Operating system weaknesses.
• Unauthorised changes to operating systems.
• Poor configuration of operating systems.
• Operating system vulnerabilities.
• Lack of an audit trail.
• Lack of an audit trail.
• Lack of segregation of duties.
• Lack of segregation of duties.

From Table 4.25 above, it is evident that IT risks are diverse and could potentially affect a wide spectrum of business processes and systems. The pervasive impact of IT risks is not only present across the general controls environment of an organisation, but also at a very granular level, in business applications. It is also key to note that the IT risk themes identified will be applicable to a varying degree, depending on the size and complexity of the organisation in question, as well as the risk tolerance level they choose to accept. A smaller organisation might, for example, buy off-the-shelf software and have no need for change or project management practices. The associated risk will therefore be irrelevant. The degree of automation and reliance on IT will also play a role. Some organisations, such as a manufacturing concern, might not have the need for extensive IT systems.

The corollary of IT risk would be to find control objectives, which are objectives or characteristics controls needed, in order to be effective in mitigating the risk. Given that controls are implemented to address IT risks, control objectives provide the opposite view of IT risk consequences, such as the availability versus the unavailability of IT systems. The following common control objectives have been repeated by a number of sources used in this section. Again, only the most frequently used control objectives are listed in Table 4.26.

Table 4.26  Frequently used control objectives (own summary)

<table>
<thead>
<tr>
<th>Control Objectives</th>
<th>Control Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality.</td>
<td>Completeness.</td>
</tr>
<tr>
<td>Integrity.</td>
<td>Validity.</td>
</tr>
<tr>
<td>Accuracy.</td>
<td>Authorisation.</td>
</tr>
</tbody>
</table>

The control objectives identified above will be used in the discussion of the link between IT risk and hacking. How the control objectives are affected by hacking will then be considered.

Thematological research questions

Based on the literature review above, the following thematological research questions can be defined:

IT risk
• The extent to which the banking sector agrees with the common IT risk themes identified.
• Determining which of the common IT risk themes are considered the most likely to take place in the banking sector.
• To determine in which order the control objectives will be ranked by the banking sector.
• To determine whether participants in the banking sector will have a difference of opinion on the IT risk themes identified.
• To determine which IT risk themes the banking sector will focus on the most.
• To determine whether the banking sector is concerned with achieving the identified control objectives.
• To determine whether the banking sector focuses on any other control objectives, over and above those identified.

4.3.6 Business continuity risk

Manmade or natural disasters are the two categories that lead to disruption of business continuity. The literature referenced in this section supports this view. Fishkin (2006:368) defines business continuity as an organisation’s ability to continue with business operations during “unusual or extraordinary circumstances”, such as hurricanes, fire, labour strikes, power outages, terrorist attacks and cyber threats, which includes the threat posed by hackers. Akin to this, Herrmann (2002:140) describes contingency planning as the plan for unanticipated, unknown events, which would call into action “alternative strategies” to continue with business operations.

The importance of business continuity has grown beyond the point of only having reactive disaster recovery processes in place. The focus is increasingly on total business continuity management, as a strategy to minimise business disruption, which falls under the umbrella of operational risk, as discussed in section 4.3.3. Doughty (2001:xi) argues that BCP has become a crucial element of an organisation’s risk management strategy. An ideal management strategy for business continuity management is provided by Young (2006:93):

Business continuity management is an all-embracing concept that covers the total spectrum of recovery from the initial response to a risk event, through to the full restoration of the business in the case of catastrophic events. Business continuity management requires a proactive approach in order to forecast potential catastrophic events, and to prepare contingency plans if such events occur. It is imperative, however, that all employees be involved in this process, as everyone has a responsibility to ensure the effectiveness of business continuity plans.

Business continuity risks are not limited to IT events. There are many possible events which could lead to a business continuity scenario. There might be an incident at a neighbouring organisation, forcing the whole area to evacuate. There might be a high demand for services, leading to a shortage of power or water. Workers might go on strike or there might be significant legal sanction against the organisation. These events could take place.
intentionally or unintentionally. Of course, IT could also play a significant role, such as system failure (Hiles, 2007:10). An organisation needs to prepare itself for any unusual information security event, including manmade events, such as malicious attacks by hackers (Wessels, 2006:3) or a significant malware outbreak.

In a study conducted by Cerullo and Cerullo towards defining a comprehensive BCP, internal and external threats from an information security perspective that may lead to a business continuity scenario were identified. Internal threats identified include hardware and software failures, system capacity constraints and internal attacks by employees (Cerullo & Cerullo, 2004:73). External threats identified include viruses and attacks by hackers (Cerullo & Cerullo, 2004:74-75). As an example, the SQL Slammer worm infected millions of computers worldwide during January 2003, disabling 13000 ATMs of the Bank of America. Total losses due to damage caused by this worm are estimated to be close to one billion dollars (Wessels, 2006:6).

To illustrate the preparedness of organisations from a BCP perspective, reference is made to a study conducted by AT&T during 2007, where 100 IT executives were interviewed from organisations where the overall annual revenue was more than $10 million. Respondents were all located in the USA. With reference to the importance of having a BCP, 26% indicated that it is not a high priority, while a similar percentage (26%) indicated that they do not have any BCP in place. In relation to the most significant threat recognised by the respondents, 45% indicated that hackers were the biggest threat. Viruses and worms were considered the biggest threat by 74% (AT&T, 2007:2, 4, 5, 9). Despite the realisation that hackers and malware are significant threats, some organisations in this survey were not prepared for any major incidents.

In King II, apart from listing business continuity risk, other references to the topic are vague, for example under the sustainability of internal control under adverse operating conditions, which implies readiness for such conditions (IoD, 2002:77). King II also specifies that new technology and IT-based operations should be subjected to the risk-based principles of availability and continuity, which again implies a mature IT environment with business continuity systems and procedures in place (IoD, 2002:84).

In the King III Report there is no reference to business continuity risk; however, business continuity is discussed a number of times in the report. The King III Report recommends a business continuity plan as a risk mitigation response (IoD, 2009b:78). It also suggested that an organisation’s IT frameworks and policies should address business continuity (IoD,
The King III Report requires a business continuity programme to ensure the successful recovery of the organisation business critical information (IoD, 2009b:86). King III lists the concept business continuity in the glossary of terms (IoD, 2009a:52; IoD, 2009b:119) and also in the definition of information security (IoD, 2009a:53; IoD, 2009b:120).

### 4.3.7 Disaster recovery risk

It is suggested that disaster recovery is considered a part of business continuity, with the difference being that it addresses the immediate consequences of an event, such as switching off a system that has been breached or assessing the damage after a natural disaster (Snedaker, 2007:586).

In the context of disaster risk, Bornman (2004:102) distinguishes between natural and manmade disasters, similar to the classification identified in section 4.3.6. Cascarino (2007:341) indicates that DRPs could be called into action due to any of the threats faced by an organisation, as presented in Table 4.27.

<table>
<thead>
<tr>
<th>Threats which may call a DRP into action (Cascarino, 2007:341)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Fire.</td>
</tr>
<tr>
<td>• Flood.</td>
</tr>
<tr>
<td>• Building collapse.</td>
</tr>
<tr>
<td>• Explosion.</td>
</tr>
<tr>
<td>• Industrial failure.</td>
</tr>
<tr>
<td>• Fire.</td>
</tr>
<tr>
<td>• Flood.</td>
</tr>
<tr>
<td>• Building collapse.</td>
</tr>
</tbody>
</table>

From the description of business continuity in section 4.3.6, it is apparent that if business continuity cannot be maintained, a DRP may be needed. BCPs or DRPs can be called into action when political events occur, markets crash, a banking crisis materialises or natural disasters take place (Van Greuning & Bratanovic, 2000:257).

These are, however, not the only scenarios which could trigger a BCP or DRP. Disaster recovery should also be considered from an IT perspective. Dolewski (2008:6) defines disaster recovery as the “IT response to a sudden, unplanned event that will enable (an) organisation to continue critical business functions until normal IT-related services can resume.” Consequently, disaster recovery risk refers to the risk associated with the process of the recovery of IT systems in the event of a disruption or disaster (Khare, 2006:291).

Hoffman (2002:44) indicates that technology-related business disruption could be caused by
two scenarios: firstly, through external disruption, where business processes could be disrupted due to the failure of an exchange or third party system; and, secondly, through system maintenance, for example, outdated software, system development delays or the impact of computer viruses. System overloads or hacker attacks are other events that could call BCPs and DRPs into action (Herrmann, 2002:140). Whereas BCPs ensure the continued operations of an organisation and will require substantial investment in aspects such as additional IT equipment to mirror existing systems to ensure effortless failover, DRPs are aimed at minimising the disruption and restoring the business services such as restoring data from backup tapes and standby systems. Business recovery through a DRP strategy will take substantially longer when compared to a BCP (Cascarino, 2007:339-340). Business continuity solutions are also favoured above disaster recovery solutions when it is considered that it is possible to leverage IT to facilitate speedy recovery. In this regard, virtualisation technologies allow easy restoration of business applications by consolidating applications and data on a single platform (IBM Corporation, 2008:5-6). Virtualisation has evolved into cloud computing, whereby organisations are outsourcing their IT systems and operations to cloud computing providers. As part of the service level agreements, disaster recovery requirements need to be specified. Essentially the cloud computing service provider becomes responsible for disaster recovery, and the client even more dependent on this services provider. Cloud computing may have cost benefits, but may also increase the disaster recovery risk (Kandukuri, Paturi & Rakshit, 2009:517, 518).

Apart from being listed as a risk in King II, no other reference is made to disaster recovery. In King III there is no direct reference to disaster recovery risk; however, disaster recovery is mentioned in the context of management’s responsibility to ensure that “business resilience” can be maintained (IoD, 2009a:40; IoD, 2009b:85). The concept disaster recovery planning is mentioned in the glossary of terms, where the concept of business continuity is explained (IoD, 2009a:52; IoD, 2009b:119).

In the case of both business continuity risk and disaster recovery risk, the impact on an organisation could be so severe as to threaten the survival of the organisation.

4.3.8 Credit risk

Most organisations are exposed to credit risk, irrespective of the size or complexity. Simply put, credit risk is the likelihood that “a borrower may fail to repay a loan” (Joosub, 2006:25). A slightly more formal definition is provided by Chibayambuya (2007:2.33), who defines it as:

The risk of a financial loss resulting from a counterparty’s inability, for whatever
reason, to fully meet its … contractual obligations.

Credit risk relates to a debtor's ability to pay back interest or capital, based on a credit agreement. When payments are delayed or not paid in full, this could create a liquidity problem for banks in particular. Credit risk is recognised as one of the single biggest reasons for bank failures (Van Greuning & Bratanovic, 2000:125; Chibayambuya, 2007:2.33; Young, 2006:3).

Much of the recent global financial crisis or "credit crunch" can be attributed to credit risk. The credit crunch started between 2004 and 2007 with the residential foreclosure crisis, when banks in the USA lent money at low interest rates to borrowers who were not necessarily creditworthy. These loans were also bundled and sold on to other banks and investors in the sub-prime market. When the interest rate started rising, these borrowers defaulted. Not only the homeowners, but also the banks and investors who bought the bundled loans were affected. The fourth-largest investment bank in the USA, Lehman Brothers, had to file for bankruptcy during September 2008, due to significant financial losses in the mortgage market (BBC MMIX, 2009). Banks started tightening their lending criteria, while raising the rates for interbank loans. Banks in financial distress could not borrow money from other banks. The banks of Iceland invested heavily in foreign economies, placing trust in the investment decisions of foreign financial institutions. When the credit crunch emerged, Icelandic banks found themselves overexposed. Overnight, the growing Icelandic economy almost totally collapsed, affecting the lives of ordinary citizens (Walt, 2008). The increase in credit risk also affected other risk types, such as liquidity risk, market risk (discussed next) and reputational risk. One particular example is that of Northern Rock bank (located in the UK), which assured its depositors that the bank was not bankrupt, but depositors feared the worst and withdrew a total of £1 billion from the bank on 14 September 2007. This was after the Bank of England announced that it would provide liquidity support to Northern Rock, which then ultimately caused the run on the bank. The bank's shares fell by 32%, also increasing its market risk. This and similar events renewed the focus on financial regulations and liquidity requirements for the banking sector (BBC MMIX, 2009; Shin, 2009:101, 102, 117-118). The increase in credit risk tarnished its reputation and also led to liquidity risk.

During August 2007, reserve banks in the biggest financial markets started to intervene to salvage the situation. Businesses and organisations in most sectors and countries were impacted by the credit crunch, which also negatively affected financial markets across the globe and led to many job losses. On 21 January 2008, the London FTSE suffered its
biggest fall in seven years. It is estimated that losses due to the credit crunch could reach
the $1 trillion mark and higher (Grant, 2007; BBC MMIX, 2009; Papagianis, 2012). The
financial institutions in the USA and the UK exposed themselves to significant mortgages
risk, since they were doing business in a product type, which was not supported by sound
financial and credit principles. Bank solvency, a decline in credit availability and damage to
investor confidence affected stock markets globally. Risk advisors failed in their duty to
prevent the overexposure. Some senior executives ignored the warning signs and acted out
of pure greed. The economies of small developing countries were destabilised (mostly in
Southeast Asia, Latin America and Russia) by the significant in- and outflow of capital. While
a few financial traders and lenders of credit benefited from the speculation, the general man
in the street is struggling with rising debt, loss of employment due to job losses and
cutbacks, and higher food prices (Share The World’s Resource, 2009). To some extent,
South Africa has also felt the impact of the global credit crunch. In an interview with Maria
Ramos, the CEO of Absa, Ramos indicated that strict adherence to Basel II requirements led
to the South African banking sector not being that severely affected by the financial crisis
(Fine, 2010). The examples above illustrate the significance of credit risk in organisations
today.

There are two references to credit risk in King II. It is listed as a business risk (IoD, 2002:31,
80) and it is listed as one of the risks banks need to focus on when managing risk (IoD,
2002:187). There is no direct reference to credit risk in King III.

4.3.9 Market risk

Market risk often derives from negative uncontrolled or unpredictable movements in a share
market risk as:

… the risk that a bank may experience a loss in (on and off) balance sheet positions
arising from unfavourable movements in market prices. It is a result of changes in
prices of equities, commodities, money, and currencies.

It is suggested that market risk is categorised as a speculative risk, where the movement of
price could lead to a loss or profit. This risk is not only attributed to market movements, but
could also be as a result of traders who “take on or get rid of those risks” (Van Greuning &
Bratanovic, 2000:189). In a volatile market environment, smaller banks might find it difficult
to accurately track and determine market risk, when they do not have sufficiently
sophisticated IT systems in place to support their business (Van Greuning & Bratanovic,
TransConstellation (2007a:11) points out that one of the characteristics of market and credit risk is that it can only be managed by a select number of specialists, who are, for example, part of the trading room (for market risk) or part of a credit committee (for credit risk). In contrast, operational risk will have to be managed across the various organisational levels. The complex nature of credit and market risk requires specialised knowledge to ensure effective management of these risks.

King II addresses market risk in two separate sections: in section 2 dealing with risk management and in Appendix 3 on a director’s legal duties (IoD, 2002:80, 187) on the same basis as for technology risk. King II also refers to the market position of an organisation, as a non-financial measure in deriving the future value of an organisation (IoD, 2002:100). There is no direct reference to market risk in King III.

Market risk could have a direct impact on the reputational risk of an organisation. A study conducted by Perry and de Fontnouvelle (2005:2) on the market reaction to operational loss announcements revealed that there is an immediate and significant impact on a firm’s market value that will negatively influence the reputation of an organisation. The recent credit crunch has shown the reality of this statement. Financial markets were in severe distress, due to banks defaulting, such as in the example provided in section 4.3.8 of Northern Rock’s share price, which fell by 32%. Therefore, market risk has a direct link with the reputational risk of an organisation.

Young (2006:5) points out that most organisations, including banks, manage reputational risk as part of credit risk. This clearly illustrates the strong link between credit risk, market risk and reputational risk.

4.3.10 Compliance risk

It is evident from the literature reviewed in this section that compliance risk covers mostly adherence to legal, regulatory requirements and associated organisational aspects, such as internal policies and ethical principles, which aid in this compliance responsibility. It may also include reporting and supervisory requirements. The Federal Financial Institutions Examination Council (hereafter FFIEC) defines compliance risk as (FFIEC, 2012):

Legal/compliance risk arises from an institution’s failure to enact appropriate policies, procedures, or controls to ensure it conforms to laws, regulations, contractual
arrangements, and other legally binding agreements and requirements.

The King III Report defines compliance risk as (IoD, 2009b:90):

Compliance risk can be described as the risk of damage, arising from non-adherence to the law and regulations, to the company’s business model, objectives, reputation, going concern, stakeholder relationship or sustainability.

The Basel Committee on Banking Supervision defines it as (Basel, 2005:7):

… the risk of legal or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organisation standards, and codes of conduct applicable to its banking activities.

Compliance risk can also be defined as the “[in]ability to meet legal and regulatory requirements” (Liebesman, 2008:58). Compliance risk is most prevalent in the financial, environmental, health and safety, and security fields. However, other fields are not excluded from the effects of compliance risk. The negative consequences of compliance risk could lead to incurring fines, shutting down business operations or even criminal prosecution (Liebesman, 2008:58-59).

It is suggested that organisations across the globe, whether in the public or private sector, have to comply with a myriad of laws and regulations, placing increased pressure on these organisations. This is not only because of the complexity of the legislation and regulation, but also because of their scope, which ranges from health and safety to labour laws and laws on international trade. Consequently, one of the characteristics of compliance risk is the complexity and effort associated with reaching the required level of compliance with applicable laws and regulations (Fishkin, 2006:370). The complexity of legislation is particularly evident from the many pieces of legislation applicable to the prosecution of hacking and cybercrime. In particular in the USA, with more than 30 pieces of legislation to consider (Etsebeth, 2003: Annexure A xix; HG.org, 2012), this would significantly increase an organisation’s compliance risk, since a board of directors will have to seek expert legal advice to assist with the preparation and prosecution of a hacking incident.

Worldwide, smaller organisations in particular feel they have reached their “saturation point” with regard to for example the amount of employment-related legislation they have to comply with (Millar, 2004). Therefore, one of the key characteristics of compliance risk is the over-regulation of various industries. It is argued that South African business in general are over-
regulated, having to comply with numerous laws and bylaws, not generally understood by the average person (Louw, 2010). The South African perspective on compliance risk is that many organisations are overburdened by the amount of legislation they have to comply with (Parsons, 2008), even though organisations such as the Compliance Institute of South Africa (2009) assist organisations with standards and benchmarks to achieve compliance. Directors of organisations are particularly burdened by this compliance responsibility, since they are required to have a general working knowledge of the applicable legislation and how it will affect their organisation (Grant Thornton, 2009). Two industries that are experiencing a lot of development and change are the banking and IT industries.

Firstly, in the South African banking sector, it is an undeniable daily requirement that numerous laws and regulations must be complied with, such as Money Laundering, Financial Intelligence Centre Act, Financial Intermediary and Advisory Services Act and Basel II. Even though it puts constraints on some banking operations, it does add to the general public’s trust of the banking sector (Chibayambuya, 2007:2.31-2.32). As a response, directors are appointing compliance officers or implementing monitoring systems and reporting to assist and overcome this compliance burden (Grant Thornton, 2009).

Secondly, the IT industry is increasingly becoming a compliance-driven industry. Particularly in the USA, legislation plays a big role in shaping the internal control processes of IT. Examples of legislation include SOX, the Health Insurance Portability and Accountability Act (hereafter HIPAA) and Basel II (Ramirez, 2006:51; Lawton, 2007:43). The IT industry is a very dynamic and fast-changing industry, which implies that in order to keep up with the legislation, a lot of effort will have to go into keeping it up to date. The chances of failure are high, which increases an organisation’s compliance risk.

It is suggested that the human element associated with complying with laws and regulations applicable to the organisation could be challenging in an organisation where the ethical culture is poor. Achieving compliance can be costly and might waste valuable resources. Organisations would want solutions to be as efficient as possible in dealing with compliance issues (Deloitte Development LLC, 2008:9). The opposite is also true, in that being compliant could save money in the future (Bentley, 2006b) by avoiding associated non-compliance costs, such as legal fees and penalties. Even when the organisation has effective information security controls in place to guard confidential data, supported by organisational policies on the appropriate use of confidential information, it is often employees who circumvent the controls and inadvertently cause a security breach (Singleton, 2006b:13).
From an IT perspective, governance and regulatory compliance today is primarily about data protection, information security and the organisation’s general control environment (Spedding & Rose, 2008:90). The IT department’s inability to upgrade systems to comply with the required laws or regulations increases the exposure and risk profile of the organisation. Or even worse, when a security breach does occur and it should have been prevented by complying with a particular piece of legislation, this would reflect very negatively on the company and increase compliance risk (Faulkner, 2007:1104, 1113, 1124).

From the literature, it is evident that IT helps improve internal control, and, ultimately, governance. Conversely, it also introduces new risks due to continued advances in technology. As a result, directors need to pay attention to the security of the organisation’s IT systems. E-business ventures introduce new fiduciary responsibilities, such as intellectual property issues and cross-border taxes. IT has also enabled more sophisticated reporting mechanisms. Then again, this has increased the demand for reporting from regulatory bodies, who expect more detailed and advanced reporting results. Directors need to ensure that they fulfill all the new requirements in order to mitigate compliance risk (Wixley & Everingham, 2005:90, 94).

Just as for technology risk, credit and market risk, King II refers only to compliance risk in the chapter on risk management and in Appendix III on directors’ legal duties (IoD, 2002:80, 187). It also requires compliance with applicable laws, regulations and supervisory requirements, as part of the internal control process (IoD, 2002:77). King II further specifies that audit committees should ensure compliance with legal and regulatory provisions (IoD, 2002:138). The King III Report highlights the significance of compliance risk in principle 6.3, which emphasises that compliance risk should be part of an organisation’s risk management processes. Subsequent paragraphs in the King III Report discuss similar requirements (IoD, 2009b:90, 91, 116).

Compliance risk is a direct threat to an organisation’s reputation (Bowers & Doot, 2006:24). In particular, financial institutions, which have to implement information security in order to be compliant with required legislation, such as the Gramm-Leach-Bliley Act (hereafter GLBA) in the USA, have to be cautious. The GLBA requires financial institutions to treat their customers’ personal information as private (Nierengarten, 2006:25). Failure to do so could lead to penalties and/or reputational damage. Or, worse still, security breaches, due to negligence in complying with required legislation, could badly scar an organisation’s reputation (Burris, 2008:28). However, this would be applicable only if data privacy breaches are reported to the media, clients, investors and shareholders. In fact, companies are often
reluctant to share information on data privacy breaches in the public domain, for fear of the reputational consequences. Companies would even go as far as not reporting data privacy breaches at all, not even to the regulators (McMillan, 2008). Similar legislation with similar ramifications has not yet been issued in South Africa.

4.3.11 The effect of risk on an organisation’s reputation

Each of the categories or components of business risk discussed above can clearly have a detrimental effect on an organisation. However, it is not only the risk itself that may have such an effect, but also the mere possibility that that such a risk can manifest itself. This phenomenon is referred to as reputational risk.

Formally, reputational risk can be defined as the “current and prospective impact on earnings and capital arising from negative public opinion”. The effect of this risk could lead to litigation, financial loss, a loss of customers and clients, and also a loss in market value. The reputation of an organisation is gained over time and has its origin in the perceptions of customers, the public or government (Bostander, 2007:8). It could also affect the opinion of shareholders and stakeholders of the organisation. Consequently, corporate social responsibility has also become a topical point, closely linked with reputational risk (Chibayambuya, 2007:2.27). A hard-earned reputation is also easily lost, making reputational risk considerably more difficult to manage than other risk types (McDowall, 2006; Perry & de Foutnouelle, 2005:4). In a survey conducted in 2005 by the Economist Intelligence Unit among 269 senior risk executives, 52% of them indicated that they regard reputational risk as more important than regulatory, human capital, IT, market or credit risk (Vallens, 2008:37). Organisations often invest substantially in building their brand; however, when the public does not experience what they portray, this could negatively affect their reputation (IMS Risk Solutions Ltd., 2003:12).

Reputational risk is increasingly being regarded as a crucial component in attracting the required capital and resource skills for an organisation. Financial scandals, terrorist attacks, natural disasters and significant IT failures could have a significant effect on an organisation’s reputation. With the increase in regulatory oversight, an organisation’s compliance risk is increasing. Subsequently, reputational risk increases due to non-compliance, cannot be ignored (Gaultier-Gaillard & Louisot, 2008:181; Regan, 2008:188, 190). As explained in section 4.3.8, the credit crunch led to a loss of investor and customer confidence. Consequently, organisations’ reputational risk was also affected. From an IT risk perspective, in an interview conducted with IT audit managers from KPMG, they indicated
that the business risk most likely to be affected by a hacking incident is reputational risk (Padayachi & Keyser, 2008). With increased focus on data privacy and the need for data security, banks have a dependency on technology to enable this need. Failure to do so increases an organisation’s reputational risk (Centre for the Study of Financial Innovation, 2010:24-25).

On the positive side, it is suggested that a strong reputation benefits an organisation in many ways. It could create higher market value and improve the organisation’s standing with the investment community, regulators and shareholders. It could lead to a greater share in the consumer market, attracting more business opportunities and creating a stronger brand. Even vendors will allow room for negotiation on price in order to be associated with a strong brand. It could also attract highly skilled individuals in the marketplace and lead to being recognised as an employer of choice (Hoffman, 2002:78). It is therefore essential that reputational risk is addressed within the realm of corporate governance and risk management (Gaultier-Gaillard & Louisot, 2008:171, 176).

As risks are so often interconnected (Olsson, 2002:62), as mentioned before, it must be recognised that reputational risk, which could be influenced by or influence most of the categories of business risks, must be considered part of a total risk management strategy under the umbrella of corporate governance. For example, physical risk can increase due to poor physical access controls, which could lead to a disclosure of company confidential information in the media, increasing the organisation’s reputational risk. Operational risk may increase due to business process failures, or can be intensified due to a striking workforce, or may be affected by failing business systems, all of which could also tarnish the reputation of an organisation. This will call into action the business continuity process of the organisation. Failure to recover successfully could further increase reputational risk. Human resource risk, realised through labour action undertaken by disgruntled employees, could create a negative perception in the market. Compliance risk, influenced by a failure to comply with regulatory requirements, can also affect an organisation’s reputation. Credit and market risk are both closely linked to reputational risk, possibly leading to the total demise of an organisation. Both technology and IT risk can increase due to hacker information security breaches that could lead to a loss of consumer confidence, thus significantly increasing the organisation’s reputational risk.
4.3.12 Conclusion

It was established in chapter 3 that hacking may be classified as an event resulting from the exploitation of a risk or risks, and that it may be classified as a risk itself. It was further established that hacking is a significant risk in the business context. After a variety of sources were considered, it was established in this chapter that the risk categories as presented in King II are a fair representation of the scope of business risk that will form the basis of the discussion of the link between the business risk categories and hacking.

This section considered the characteristics of each of the risk categories, highlighting the difficulty of attributing one definition to each considering some of the overlaps between the risk categories. On its own, physical risk relates to the exposure of the organisation’s assets to a range of threats, including natural disasters and unauthorised access. Advances in technology have shifted the boundaries of physical risk to multiple locations that may not even be under the full control of the organisation due to the mobility of technology. Information and data assets of organisations will be particularly at risk. Operational risk is closely related to the business operations of an organisation and includes issues related to people, processes, technology and external factors. By implication, it affects many aspects within an organisation, importantly also IT. Human resource risk addresses risks associated with employee actions, behaviours and human resource practices, such as training, skill levels, productivity and availability of resources. Technology risk can be viewed as a collective term for advancement in technology in the broader sense, but importantly includes IT risk. IT risk can be defined or characterised in a range of ways, as is evident in Table 4.25. But, in essence, it includes the following risks: unauthorised logical and physical access, business and IT disruption, lack of compliance, irregularities, theft and fraud, cybercrime, inadequate IT operations, lack of project management practices, data interception, a lack of segregation of duties, application input, processing and output weaknesses, communication and interface failures, and changes or theft of data, systems or programmes. In addition, the following control objectives have been identified: confidentiality, integrity, availability, accuracy, completeness, validity, security and authorisation. A control objective will help ensure that controls defined as part of the response to hacking achieve their desired objective.

As regards the remaining categories of risk, business continuity and disaster recovery risk are related to the risk of loss or disruption to an organisation, including the organisation’s preparedness for business continuity events. Credit risk relates to the risk of a counterparty not meeting its contractual obligations, while market risk is the risk of losses to the market
due to movements in those markets. Compliance risk refers to the consequences associated with non-compliance with laws, regulations and policies, while reputational risk addresses the effect on an organisation of other perceived risks.

Through the literature review conducted in this chapter, the pervasive nature of IT across all spheres of the organisation has been considered. When taking the conclusions of chapter 3 into consideration, where the importance of hacking within the business context has been highlighted, the next step would be to explore the links between hacking and IT risk, as well as the control objectives. This will be followed by the links with the business risks discussed in this chapter.

4.4 THE LINK BETWEEN HACKING, IT RISK AND CONTROL OBJECTIVES

The analysis of the different meanings of IT risk presented in section 4.3.5.4 to 4.3.5.17 leads to the documentation of common IT risks and control objectives that characterise IT risk in Tables 4.25 and 4.26. These characteristics of IT risk and control objectives will now be used to explore the link between hacking (as discussed in chapter 3) and IT risk, to show the pervasive nature of hacking in IT. A summary of the links between IT risk and hacking will be presented in Table 4.28, while the link between hacking and control objectives will be presented in Table 4.29. This will assist with the discussion of the pervasiveness of hacking in business.

4.4.1 The link between hacking and IT risk

Each IT risk can be closely linked with hacking attack types. Each IT risk theme will be briefly discussed in turn:

- **Unauthorised physical access and the lack of physical access control and security.** From a physical access perspective, as explained in section 3.8.3, hackers may use social engineering techniques (such as tailgating) to gain access to an organisation’s premises. Once access has been obtained, hackers may place a key logger or sniffer to capture information. They may also install backdoors and Trojans on PCs, to obtain access remotely. Or, they may even simply use a USB device to remove data. Hackers also use wardriving to find open and vulnerable wireless networks (as presented in section 3.8.3.3 and 3.9.1.1).

- **Lack of compliance with IT policies, procedures, legal and regulatory requirements.**
Hackers, of course, show a total disregard for an organisation’s policies and procedures and the laws of the target being attacked, as explained in section 3.5.2 and 3.8.7. Employees inside an organisation (insiders) might also show a total disregard for the organisation’s policies and procedures, as explained in section 3.5.3.6.

- **Business and IT disruption.** Hackers use various attack types to cause major disruption, such as DoS attacks (sections 3.3.2, 3.5.3.1, 3.5.3.2, and 3.9.1.1), malware such as viruses and worms (sections 3.5.3.1, 3.5.3.2, 3.9.6 and 3.10.1) and web defacements (sections 3.2.3, 3.6, 3.10.1 and 3.13).

- **Inadequate IT operations and support.** Hackers can take advantage of inadequate IT operations and support, where for example, a particular system receives minimal support, leaving it vulnerable to an attack. Hackers also prey on poor IT operational processes, such as a weak helpdesk support function, and use social engineering attacks, as discussed in sections 3.6 and 3.9.1.2.

- **Theft or damage to IT equipment.** Hackers might steal data, information or IT equipment for financial gain, as discussed in section 3.5.3.6 and 3.9.4. Hackers with malicious intent will physically damage IT equipment once inside an organisation, as discussed in section 3.8.2, 3.9.4 and 3.11.2.

- **Inadequate change and project management practices.** Hackers can also take advantage of poor change control processes, where unauthorised software is loaded into the production environment, as discussed in section 3.8.5. Hackers, and in particular insiders, could load malicious or altered code into the production environment, leading to the fraudulent processing of transactions or interference with normal operations, as reflected on in sections 3.5.3.6 and 3.8.3.1. Poor software development practices, such as inadequate testing, may also lead to vulnerabilities which are exploited by hackers (covered in sections 3.8.5 and 3.9.2).

- **Misuse of IT, irregularities and fraud.** By nature, hacking is the misuse of IT, through highly irregular means (such as establishing IRCs or storing illicit material), often leading to some sort of fraud, as discussed in sections 3.4, 3.5.2 and 3.5.3.6.

- **Cybercrime.** Hacking is a form of cybercrime and is also related to other forms of cybercrime, such as theft of data, use of malware, phishing, electronic banking fraud,
blackmailing, corporate espionage and cyberterrorism (Colarik, 2006:42; Gordon & Ford, 2006:14-15), as was extensively discussed in section 3.10.1.

- **Unauthorised logical access.** One of the most commonly used hacker attacks is password attacks, as discussed in sections 3.9.1.1 and 3.9.2. Various attack techniques exist to circumvent logical access, ranging from offline password attacks to using social engineering to obtain user credentials.

- **Inadequate IT performance, inefficient use of IT resources, human resources deficiencies and complexity of IT** are discussed. These are mostly related to poor organisational processes, which can be exploited by hackers through, for example, social engineering attacks (discussed in sections 3.8.7 and 3.9.4). DoS attacks could affect the performance of IT (section 3.9.1.1) and software vulnerabilities introduce a layer of complexity in IT, as argued in section 3.8.5.

- **Application control weaknesses.** Web applications in particular are vulnerable to hacker attacks. Web application input often lack input validation controls, as discussed in section 3.9.3, which may lead to errors, unauthorised transactions or application manipulation. Web application sessions could be interrupted via session hijacking or attack session management, as discussed in section 3.9.1.1 and 3.9.3. Transaction logs or audit trails of a web-application could be changed or erased to cover fraudulent activities, as discussed in section 3.6.

- **Data control weaknesses.** Hacker attacks often lead to theft, loss or damage to data, systems and programmes, as discussed in sections 3.3.3, 3.3.5, 3.5.3.1, 3.6, 3.8.3.2, 3.9.1.1 and 3.9.4. A popular technique used by hacker to obtain data is SQL injection, as explained in section 3.9.3.

- **Interface control / network weaknesses.** Various hacker attacks can lead to communication or interface failures, such as DoS (section 3.9.1.1), targeted router attacks (section 3.8.6), session hijacking, ARP spoofing and network level attacks (sections 3.9.1.1 and 3.9.1.2).

- **Operating system weaknesses.** Various hacker attacks focus on operating system weaknesses, such as port scanning, vulnerability scanning, buffer overflow exploits, stopping operating system services, exhausting resources, backdoors / rootkits, DoS (all discussed in section 3.9.1.1), environmental variable manipulation, exploiting
insecure configuration and unauthorised remote access (all discussed in section 3.9.1.2).

- **Lack of audit trail.** Black hat hackers often compromise one system to achieve anonymity, when attacking other platforms, as discussed in section 3.3.5. This activity will take place unbeknownst to the system administrator, if no audit trail or log is kept of suspicious activity. A hacker would also delete or alter the log file, during the maintenance phase of the hacker methodology, as discussed in section 3.6.

- **Lack of segregation of duties.** Hackers can collaborate with an insider to gain access to network resources, systems or data, as discussed in sections 3.5.3.6 and 3.12.3. Hackers often escalate their system privileges as soon as they have successfully hacked into a system, as discussed in section 3.6.

Based on the analysis above, there are different types of hacker attacks that can be associated with the common IT risks (summarised in Table 4.28).

<table>
<thead>
<tr>
<th>Table 4.28</th>
<th>Linking common IT risk themes with hacking attack types (own summary)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Common IT risk themes</strong></td>
<td><strong>Hacking attack types</strong></td>
</tr>
<tr>
<td><strong>General controls</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Unauthorised physical access / Lack of physical access control and security. | • Social engineering.  
• Key loggers / USB.  
• Backdoors / Trojans.  
• Sniffers.  
• Wardriving. |
| Lack of compliance with IT policies and procedures, legal and regulatory requirements. | Hackers show a total disregard for IT policies and procedures, and the countries cyber laws. |
| Business and IT disruption. | • DoS.  
• Malware.  
• Web-defacement. |
| Inadequate IT operations and support. | Social engineering |
| Theft, loss or damage to IT equipment. | • Theft of removable media, computer components and laptops.  
• Malicious damage to equipment. |
| Inadequate change / project management practices. | • Malicious code deployment.  
• Exploiting software vulnerabilities. |
| Misuse of IT / Irregularities and fraud. | • IRC.  
• Illegal storage of tools and illicit material. |
| Cybercrime. | Hacking is a form of cybercrime. |
| Communications failure / Intercepting data during transmission. | • Sniffers.  
• Session hijacking.  
• ARP spoofing. |
| Unauthorised logical access. | • Passive online attacks. |
Common IT risk themes | Hacking attack types
---|---
• Inadequate IT performance.  
• Inefficient use of IT resources.  
• Human resources deficiencies.  
• Complexity of IT.  | • Active online attacks.  
• Offline attacks.  
• Non-electronic attacks / social engineering.  
• Social engineering.  
• DoS-attacks.  
• Software vulnerabilities.
Application controls  
• Application control weaknesses. | • Input validation weaknesses.  
• Session hijacking.  
• Attack session management.
• Data control weaknesses. | • Theft of data and programmes.  
• Alteration of data and programmes.  
• SQL injection.
• Interface control / network weaknesses. | • Sniffers.  
• DoS.  
• Targeted router attacks.  
• Session hijacking.  
• ARP spoofing.  
• Network level attacks.  
• Session hijacking.  
• Network level hijacking.
• Operating system weaknesses. | • Port scanning.  
• Vulnerability scanning.  
• Buffer overflow exploits.  
• Stopping services.  
• Exhausting resources.  
• Backdoors / rootkits.  
• Environmental variable manipulation.  
• Exploiting insecure configuration.  
• Unauthorised remote access.  
• DoS.
• Lack of audit trail. | • Alteration of web-application logs.  
• Alteration of operating system logs.
• Lack of segregation of duties. | • Collaboration with insider.  
• Escalation of privileges.

### 4.4.2 The link between hacking and control objectives

Now that the link between hacking and the common IT risk themes has been provided, the attention turns to the control objectives identified in section 4.3.5.17:

- The control objective *confidentiality* can be challenged by many hacker attacks, such as password attacks, sniffing, session hijacking (discussed in section 3.9.1.1 and 3.9.2), which may give access to confidential information. Non-technical techniques, such as theft of mobile devices, could also compromise confidentiality (covered in
Confidential data can also be used by a hacker via social engineering attacks to gain access to a system as a legitimate user (discussed in sections 3.8.7 and 3.9.4).

- The control objective **integrity** can be compromised when a hacker alters event logs to hide his activity, or compromises data integrity by intentionally or unintentionally damaging or altering files or data on the target system, as discussed in sections 3.9.3 and 3.13.

- The control objective **availability** in particular is compromised during DoS attacks. An organisation’s operations can come to a complete standstill, as pointed out in sections 3.9.1.1 and 3.13. Web application attacks, such as web defacement, might also affect the availability of an organisation’s online presence, as discussed in section 3.9.3.

- The control objective **accuracy** can be affected by attacks, such as race conditions, which may affect the outcome of application logic, manipulating business transaction processing, bypassing client-side controls, such as manipulating URL parameters, affecting the accuracy of, for example, online purchases being authorised, as discussed in section 3.9.3.

- The control objective **completeness** can be compromised by attacks such as IP address spoofing, where data is lost during transmission, due to the redirection of traffic. Session hijacking could also result in a user being unable to complete his transaction, since the hacker took control over the transaction session in progress. Both of these attacks were discussed in section 3.9.1.1.

- The control objective **validity** can be compromised by attack types, such as attacking application logic, which exploits vulnerabilities in the application, which may affect the validity of applications being processed. This could alter transactions at a business process level (discussed in sections 3.3.5 and 3.13). Attack session management compromises the validity of a user session, allowing the attacker to use the web application as a valid user. Both of these attacks were discussed in section 3.9.3.

- The control objective **security** can be affected by many hacker attacks. Physical security can be compromised through, for example, gaining unauthorised access to an organisation’s premises and wardriving, as discussed in sections 3.6, 3.8.3 and 3.9.4.
Logical access security can be compromised via, for example, password attacks, wardialling and installation of backdoors (discussed in sections 3.8.4, 3.9.1.2 and 3.9.2).

- The control objective *authorisation* is compromised in many attack types, due to the nature of hacking activity. Hackers do not seek authorisation when attacking a target system, as highlighted in sections 3.2.4 and 3.3.5. This could circumvent transaction authorisation at a business process level (discussed in sections 3.5.3.6 and 3.6). Hackers will store their data, tools and illicit material on the target which has been breached, without authorisation from the system owner, as explained in section 3.6.

Clearly, there are different types of hacker attacks that can be associated with the common control objectives (summarised in Table 4.29).

**Table 4.29** Linking control objectives with hacking attack types (own summary)

<table>
<thead>
<tr>
<th>Control Objective</th>
<th>Hacking attack type examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>- Password attacks.</td>
</tr>
<tr>
<td></td>
<td>- Sniffing.</td>
</tr>
<tr>
<td></td>
<td>- Session hijacking.</td>
</tr>
<tr>
<td></td>
<td>- Phishing.</td>
</tr>
<tr>
<td>Integrity</td>
<td>- Alteration of web-application logs.</td>
</tr>
<tr>
<td></td>
<td>- Alteration of operating system logs.</td>
</tr>
<tr>
<td></td>
<td>- Alteration of data and programmes.</td>
</tr>
<tr>
<td>Availability</td>
<td>- DoS.</td>
</tr>
<tr>
<td></td>
<td>- Malware.</td>
</tr>
<tr>
<td></td>
<td>- Web-defacement.</td>
</tr>
<tr>
<td>Accuracy</td>
<td>- Alteration of data and programmes.</td>
</tr>
<tr>
<td></td>
<td>- Race conditions.</td>
</tr>
<tr>
<td></td>
<td>- Manipulation URL parameters.</td>
</tr>
<tr>
<td>Completeness</td>
<td>- IP address spoofing.</td>
</tr>
<tr>
<td></td>
<td>- Session hijacking.</td>
</tr>
<tr>
<td>Validity</td>
<td>- Attack application logic.</td>
</tr>
<tr>
<td></td>
<td>- Alteration of data and programmes.</td>
</tr>
<tr>
<td></td>
<td>- Input validation weaknesses.</td>
</tr>
<tr>
<td></td>
<td>- Attack session management.</td>
</tr>
<tr>
<td>Security</td>
<td>- Bypass physical access.</td>
</tr>
<tr>
<td></td>
<td>- Password attacks.</td>
</tr>
<tr>
<td></td>
<td>- Wardriving.</td>
</tr>
<tr>
<td></td>
<td>- Wardialling.</td>
</tr>
<tr>
<td></td>
<td>- Web application attacks.</td>
</tr>
<tr>
<td></td>
<td>- Sniffing.</td>
</tr>
<tr>
<td></td>
<td>- Backdoors.</td>
</tr>
<tr>
<td>Authorisation</td>
<td>- All hacker attacks and access into systems are unauthorised in nature.</td>
</tr>
<tr>
<td></td>
<td>- Unauthorised storage of data and illicit material.</td>
</tr>
</tbody>
</table>

The presentations in Tables 4.28 and 4.29, linking IT risk and hacking, demonstrate the
diversity of hacker attacks and the pervasive impact of hacker attacks on business, in particular in respect of IT risk and the related control objectives. Hacking incidents affect IT systems that the business relies on for its daily operations. Therefore, indirectly, hacking incidents impact the business’s ability to survive and increases its reputational risk. However, it is not only IT risk and reputational risk that is impacted, but indeed all of the risk categories.

Hacking is not only pervasively associated with IT risk, but can also be strongly related to the each business risk type identified in this thesis. This chapter now explores the link between hacking, IT risk and each business risk type in turn.

**Thematological research questions**

Based on the literature review above, the following thematological research questions can be defined:

**IT risk**
- The extent to which there is an understanding within the banking sector of the direct link between hacking and IT risk.
- The extent to which there is an understanding in the banking sector that each control objective defined by management could be compromised by hacking.

**Hacker threat**
- The extent to which there is an understanding within the banking sector of the diversity of hacker attacks.
- The extent to which the hacker attack types have caused the common IT risk themes to materialise in the banking sector.
- The control objectives set by management in the banking sector and the monitoring of the hacker threat, which could jeopardise those objectives.

For easy referencing, the common IT risk themes identified in Table 4.26 will be highlighted in *italics* in the sections that follow.

### 4.5 THE LINK BETWEEN HACKING, IT RISK AND PHYSICAL RISK

Physical risk relates to the exposure of the organisation’s assets to a range of threats including natural disasters and unauthorised access, obviously manifesting through either natural or manmade events.

Due to the pervasiveness of IT servers and networks, physical access risk needs to be addressed in all areas of the business, as discussed in section 4.3.2. It was indicated in sections 3.6 and 3.8.3.1 that hackers might make use of social engineering, such as stealing
an access card, tailgating or impersonating an employee, to gain unauthorised physical access. This could lead to physical damage to IT equipment by hackers, or even theft of IT equipment or removable media, as noted in sections 3.8.3.1, 3.10.1 and 3.13. Physical damage to IT equipment and networks by hackers could lead to disruption of IT and business operations, as a result of the increase in physical risk, as highlighted in section 4.3.2. It was explained in this thesis how hackers may look for unattended PCs to get access to the network to steal or damage confidential data or applications. Unauthorised access to IT systems may also be accomplished via shoulder surfing, which occurs when a user is observed entering a password. These attack techniques were discussed in sections 3.9.2 and 3.9.4. Hackers might even place a key logger or install sniffer software to capture user credentials. They might browse around open shared workspaces, looking for information on the configuration of networks, web servers and firewalls, as explained in section 3.8.3.1. These examples also illustrate how hacking affects the control objectives confidentiality, authorisation, security, availability and integrity (as identified in section 4.3.2), which strongly relates to physical risk.

It was argued in section 4.3.2 that physical risk expands beyond the physical boundaries of an organisation. These vulnerabilities are exploitable due to a lack of physical access control and security. Firstly, hackers may engage in dumpster diving as part of hacker reconnaissance, to find confidential information which might assist them in planning their attack, as explained in section 3.6, 3.9.1.1, 3.9.1.2 and 3.13. Secondly, hackers might exploit an organisation’s wireless network by making use of wardriving, as explained in sections 3.6 and 3.8.3.3. Thirdly, hackers might target mobile technologies, ranging from USB storage devices to smartphones, which might contain confidential information, as discussed in section 3.8.3.2 and 3.8.7. Therefore, weaknesses in physical access controls, which increase the physical risk, will also increase IT risk, due to the likelihood of theft or damage to IT equipment. This will also increase the likelihood of hackers gaining access to sensitive information, without having to deploy sophisticated automated attacks.

A hacker from outside of the organisation will have to breach the physical security of the organisation. In contrast, insiders who already have access (as discussed in section 3.5.3.6), might be able gain entry into more sensitive areas (inappropriate staff access as highlighted in section 4.3.2), such as the organisation’s data centre, which should also be considered from physical risk perspective.

Although physical risk can be mitigated partially through implementation of physical security measures, the human element is often the reason why these mechanisms fail. It remains
undisputable, however, that physical access remains the board of director’s first line of
defence against hackers and other likeminded individuals.

**Thematological research questions**

Based on the literature review above, the following thematological research questions can be defined:

**Business risk**
- The extent to which there is recognition in the banking sector of the existence of the link between hacking, IT risk and physical risk.
- The extent to which there is a recognition that IT risk extends beyond the physical boundaries of banks.
- The extent to which the banking sector is protected against physical risk inside a bank.

**Hacker threat**
- The extent to which the banking sector is vigilant against physical hacker attacks.

### 4.6 THE LINK BETWEEN HACKING, IT RISK AND OPERATIONAL RISK

As discussed in section 4.3.3, operational risk is closely related to the business operations of an organisation and speaks to people, processes, technology and external factors such as regulations and external competition. Each of these focus areas has unique risks, although at the same time they are interdependent.

The people component of operational risk relates to losses incurred due to the actions of employees. The people component is therefore closely related to human resource risk, which will be expanded upon in section 4.7. Many would argue that a business is only as strong as its people. A business cannot operate without the skills and support of its employees. Human resource deficiencies increase both IT risk and operational risk. Employees are often the root cause of realising some of the common IT risk themes identified in section 4.3.5.17. For example, employees could fail to comply with the organisation’s IT policies and procedures. The “human factor” is also often the driver behind successful hacking attempts, as discussed in section 3.8.7. The risk associated with the people component of operational risk increases when employees ignore the organisation’s clean-desk policy. Sensitive or confidential information, including user credentials, might be lying around, allowing hackers to obtain information, which may assist them in gaining unauthorised logical access to the organisation’s systems, as discussed in section 3.8.4.

Employees might also be responsible for the common IT risk theme theft, loss and damage to IT equipment. Insiders might use their existing system privileges to gain unauthorised
physical access to the organisation’s systems, as explained in section 3.5.3.6, compromising the organisation’s security. Employees might be responsible for the misuse of IT, such as excessive use of the Internet for personal entertainment, or downloading hacker tools (as mentioned in section 3.5.3.6), which might in turn be used to breach the organisation’s systems. The control objectives affected by the people component of operational risk include confidentiality, security and authorisation. The people component of operational risk can therefore significantly increase IT risk, which in turn could also increase the likelihood of hacker and insider attacks.

The process component of operational risk relates to possible failure of business processes, compromising availability. IT has automated numerous manual business processes, creating greater efficiencies for organisations. At the same time, IT has also introduced numerous new risks, such as the common IT risk themes associated with applications. The common IT risk theme inadequate project management practices may lead to the delivery of inferior and risk-prone software solutions. Software vulnerabilities might be introduced into business applications (creating application and data control weaknesses), providing hackers with possible weaknesses to exploit, as explained in section 3.8.5. Weaknesses in operational business processes, leading to inadequate IT operations and support, could be exploited by hackers to allow them access into the organisation’s network. For example, using social engineering techniques, weak helpdesk procedure might be exploited to insist on a password reset, as explained in sections 3.6, 3.8.7, 3.9.1.2 and 4.4.1. The control objectives affected by the process component of operational risk includes availability, accuracy and validity.

The technology component of operational risk focuses on the impact of technology on organisations in general, and more specifically, the pervasive effect of IT on business. IT provides the support business requires in order to remain competitive in a global marketplace. Without operational IT systems and processes, business failure is probable. Communication failures due to a hacker DoS attack and IT performance issues are some of the technology issues organisations have to grapple with. IT risks are primarily linked to the technology component of operational risk, as a category of business risk, as pointed out in section 4.3.3.

Highly complex technological environments, such as banking institutions, are what hackers thrive on, as considered in section 3.5.1. The board of directors and senior management, on the other hand, do not always clearly understand the complexities of their organisation’s IT systems. Hackers see this as a challenge or opportunity, exploiting the control weaknesses
that occur within business processes and applications. In section 3.12.3, this study indicated that hacker attacks have led to significant financial losses for both the banking sector and customers alike.

Web applications that might have been developed without validation controls could introduce application control weaknesses, which compromises transaction validity and integrity. As discussed in section 3.9.3 of this thesis, hackers might use web attack techniques to break into web applications. A further consequence could be that a hacker attack could intentionally or unintentionally lead to the IT risk of business and IT disruption, as concluded in section 3.3.2 and 3.6. Hackers could exploit data control weaknesses, or compromise the integrity of data transmitted across the network. Business processes might be affected as a result. Hackers may exploit operating system weaknesses, granting them access to business applications and data. The control objectives affected by the technology component of operational risk include completeness, accuracy, integrity and authorisation.

The external factors component of operational risk focuses on factors that are often beyond the control of the organisation. Consideration should be given to cybercrime, an IT risk that also includes hacking, as noted in sections 3.10 and 4.3.3. Another external factor to consider is legislation, which might bring the IT risk lack of compliance with regulatory requirements into effect (further explored in section 4.11).

It can also be argued that hacking affects all four components of operational risk simultaneously. For example, a hacker could successfully break into a critical business application. In the process, the operating system configuration is corrupted and needs to be restored (technology). The organisation’s business process halts, because of the reliance on the critical business application (processes). As a consequence, the IT risk business and IT disruption has materialised (discussed in more detail in section 4.9). The productivity of employees is affected and IT personnel have to spend valuable time restoring the business application (people). The media reports the hacker incident and regulatory bodies investigate the possibility of a data privacy breach (external factors). It is clear from this example how the people, processes, technology and external factor components of operational risk are affected by a hacker attack.
Thematological research questions

Based on the literature review above, the following thematological research questions can be defined:

**Business risk**
- The extent to which there is recognition in the banking sector of the existence of the link between hacking, IT risk and operational risk.
- The extent to which hacking as a risk is evident in each of the four components of operational risk, within the banking sector.

4.7 THE LINK BETWEEN HACKING, IT RISK AND HUMAN RESOURCE RISK

As discussed in section 4.3.4, human resource risk involves the risks associated with employee actions, behaviours and practices, including issues related to skill levels, productivity and availability of resources.

An organisation cannot function without competent staff. Without talented management (a human resource risk factor identified in section 4.3.4), the organisation might fail to attract and retain competent staff (a factor to be considered as part of the IT risk human resource deficiencies). Poorly skilled network administrators might fail to maintain the organisation’s systems, due to a lack of training or development initiatives in the organisation. This could also be due to poor project and software development practices. This may introduce software vulnerabilities (one of the primary weaknesses that facilitate successful hacking attempts, discussed in section 3.8.5) that hackers might exploit. The unavailability of key staff to perform critical updates to systems when zero-day vulnerabilities have been identified could expose the organisation to hacker attacks. This could lead to business and IT disruption.

Human behaviour and emotions play a key role in an organisational context. Humans often tend to act on emotions, as discussed in section 4.3.4. This may lead to errors, malicious or unauthorised actions on part of the employees, compromising the integrity, validity or accuracy of IT system processing. Again, this speaks to the IT risk human resource deficiencies. This behaviour might also introduce system configuration errors or vulnerabilities, exploitable by hackers. Another aspect of human behaviour is employees who are in financial trouble and who may be tempted to commit fraud, a factor that increases people risk, as discussed in section 4.3.4. This in turn relates to the IT risk misuse of IT, irregularities and fraud. Hacking could be a means of committing fraud, in particular by insiders, as mentioned in section 3.5.3.6.
The introduction of new IT solutions creates uncertainty, particularly in the user community, as discussed in section 4.3.4. Employees tend to show resistance when having to learn new software applications or IT solutions (also part of the IT risk human resource deficiencies). When opting for outdated IT solutions or software to appease the technology resistance by employees, hackers may use this to their advantage, since older software may contain known security weaknesses, as discussed in section 3.8.5. The introduction of new IT solutions, on the other hand, may introduce new IT complexities and vulnerabilities, which are also exploitable by hackers. This also increases the organisation’s IT risk.

The discussions in this thesis have indicated that the human element is a significant contributor to the likelihood of successful hacking attacks. Employees would rather write down a complex password than make the effort to memorise it. Hackers are opportunistic in nature and would always be on the lookout for the odd password lying around, as discussed in section 3.8.7, leading to the IT risk unauthorised logical access. Hackers would also use other social engineering techniques, such as impersonating legitimate users, to gain access to systems and networks. With reference to the emotional element highlighted in the literature, Mitnick (2003:20) points out that employees are often the “weakest link” in an organisation, allowing hackers to obtain confidential information from them through social engineering techniques and gentle persuasion, as discussed in section 3.8.7. He recommends that organisations should be vigilant, and should ensure that each employee takes ownership of the risk of social engineering. This strategy will decrease the organisation’s human resource risk.

Even from an insider perspective, the risk factors associated with human resource risk (identified in section 4.3.4), such as social recognition, vigilantism or revenge for discrimination, harassment, or unfair dismissal can become the motives behind their behaviour. When colluding with syndicate members outside of the organisation, as explained in section 3.5.3.6, the IT risk of the organisation also increases. The insider could override controls or create backdoors to allow hackers from syndicates to access the organisation’s systems unhampered. Not only does this realise the IT risk identified in section 4.3.5.17 unauthorised logical access, but it could also introduce data control weaknesses and even business and IT disruption. Due to a lack of segregation of duties, the risk of insiders might be hard to deter, leading to the processing and authorisation of unauthorised transactions.

The IT risk lack of compliance with IT policies, procedures, legal and regulatory requirements relates to human resource risk from the perspective of employees either neglecting to follow them or deliberately not complying with them. For example, the system...
administrator might ignore the password policy and choose easy-to-remember passwords. Hackers may use password crackers, as discussed in section 3.3.3, 3.6, 3.8.4 and 3.9.2, to obtain access via these weak logical access controls. When caught, disciplinary action might be taken against the system administrator. By not having information security policies and procedures in place, the organisation will have no recourse against these employees (compliance risk). The control objectives affected by human resource risk include integrity, validity, accuracy, availability, security and authorisation. Therefore, the risks associated with the human element as a result of IT risk could increase an organisation’s operational risk and also increase the likelihood of hacker attacks.

<table>
<thead>
<tr>
<th>Thematological research questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Based on the literature review above, the following thematological research questions can be defined:</td>
</tr>
<tr>
<td><strong>Business risk</strong></td>
</tr>
<tr>
<td>• The extent to which there is recognition in the banking sector of the existence of the link between hacking, IT risk and human resource risk.</td>
</tr>
<tr>
<td>• The extent to which the IT risks are realised, due to human resource risk, in turn increasing the likelihood of hacker attacks in the banking sector.</td>
</tr>
</tbody>
</table>

4.8 THE LINK BETWEEN HACKING, IT RISK AND TECHNOLOGY RISK

Technology risk relates to the advances, complexities and threats associated with technology (Olsson, 2002:175). The concept of technology risk has been explored in section 4.3.5. It has been indicated how both old and new technologies affect organisations. The discussions related to technology have shown how vulnerabilities and threats increase technology risk. It has further been established in section 4.3.5.4 that IT risk is a sub-component of technology risk, whilst technology risk is a broader overarching concept. It has also been established that technology risk relates to systems, a subcomponent of operational risk. More importantly, though, in the context of this thesis is the close relationship between technology risk and IT risk.

The literature review of IT risk concluded with the identification of generic IT risk themes in section 4.3.5.17. The number and variety of IT risks are pervasive across an organisation, exacerbated by continuous development and growth on the technology front. The common IT risk themes (19 in total) identified in section 4.3.5.17 will all be relevant under the category of technology risk, due to the strong link with IT risk. Similarly, all the control objectives presented in section 4.3.5.17 also relate to technology and IT risk.
Section 4.4.1 presented the link between each of the 19 IT risk themes and hacking. It has been shown that the impact of hacking is significant from an IT risk perspective. Since there is a strong link between IT risk and technology risk, it naturally follows that hacking would also increase technology risk. Indeed, hacking can also affect technology risk directly, as highlighted in section 4.3.5.

<table>
<thead>
<tr>
<th>Thematological research questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Based on the literature review above, the following thematological research questions can be defined:</td>
</tr>
</tbody>
</table>

**Business risk**
- The extent to which there is recognition of the existence of the link between hacking, IT risk and technology risk in the banking sector.

### 4.9 THE LINK BETWEEN HACKING, IT RISK, BUSINESS CONTINUITY AND DISASTER RECOVERY

Section 4.3.7 concluded on the close relationship between business continuity and disaster recovery. Whereas business continuity relates to an organisation’s ability to continue with business operations after natural or manmade disasters or interruptions, disaster recovery is called into action to ensure systems are restored to the original state. Closely linked to both these matters is the common IT risk of *business and IT disruption*. Slay and Koronios (2006:5) argue that organisations are heavily reliant on IT platforms to continue their business operations. Slay and Koronios (2006:5) go on to explain that most organisations are anxious that a loss of IT operations could lead to total business disruption, necessitating the activation of the BCP.

Several IT risks could lead to a business recovery scenario. For example, the unavailability and instability of the back-up or recovery servers will have a detrimental effect on an organisation’s ability to recover during a natural or manmade disaster. Failure to equip the backup servers with uninterruptible power supply (hereafter UPS) increases the business continuity risk (McManus & Carr, 2001:4-6). Failure to test the equipment regularly, included under the common IT risk theme of *business and IT disruption*, could also increase the business continuity risk. Hackers can either cause or benefit from these failures.

Business continuity is most often associated with natural events, such as floods or earthquakes. However, manmade events could be just as devastating. From an IT risk
perspective, a hacking incident could lead to a business continuity scenario, as explained by Ross (2008:9):

A hack, a virus or a denial-of-service attack may have the effect of halting business operations. A senior-level crisis management team that is not versed in the demands of dealing with a technical incident is likely to either panic or abdicate control. Developing a plan that can be tested and improved over time will result in a smoother, more coordinated response.

The risk posed by hackers could also lead to a business recovery scenario. A hacker attack such as a DoS attack on an organisation’s critical network infrastructure could result in prolonged business disruption (BERR, 2008:29). An inability to stop the attack or call the BCP into action could cause the situation to spiral out of control. The availability of a recovery site is also essential for the recovery of critical business services. It is not unlikely that hackers would try to access the recovery site, in particular when access control is weak. Customers of the organisation might be unable to reach the online services offered by the company. This could threaten the existence of the organisation, causing a significant business risk. With the realisation that no system is immune to a hacker attack, a risk management strategy to identify vulnerable IT components and implement IT security control measures to prevent attacks (Lipson & Fisher, 2000:35) must be put in place, and it must obviously be commensurate with the risk profile of each organisation.

Apart from an organisation’s own systems, hackers could also attack the supporting infrastructure and utilities which organisations depend on, crippling basic services – for example, electricity or telecommunications services (Blum, 2005). This could escalate into total business disruption, should the organisation have no back-up utility infrastructure to depend on, such as power generators and water storage tanks, effectively increasing the organisation’s business risk. Therefore, this is an external risk in the realm of operational risk that must be addressed as part of business continuity and disaster recovery. The control objective affected by business continuity and disaster recovery is availability.

### Thematological research questions

Based on the literature review above, the following thematological research questions can be defined:

**Business risk**

- The extent to which there is recognition of the existence of the link between hacking, IT risk and business continuity and disaster recovery in the banking sector.
- Whether the banking sector considers the likelihood of a hacker attack leading to a business continuity scenario.
• Whether the banking sector considers the IT risks, which may be exploited by hackers and could lead to a business continuity scenario.

4.10 THE LINK BETWEEN HACKING, IT RISK, CREDIT AND MARKET RISK

As discussed in section 4.3.11, credit and market risk is inextricably linked to the reputational risk of an organisation. When the reputation of an organisation is negatively affected, this will affect its position in the market, as well as its ability to obtain credit.

Vallens (2008:37) argues that numerous studies have shown that organisations with a “strong positive reputation have higher market value”. As much as 75% of an organisation’s value can be attributed to reputation. Perry and de Foutnouvelle (2005:2) have also indicated that operational losses occurring inside an organisation have a significant impact on the firm’s market value and consequently also impact its reputation. Credit risk is also linked with reputational risk, in particular when organisations do business with companies that have poor credit ratings (Vallens, 2008:37). Since there is this strong link between credit and market risk and reputational risk, an event that affects the reputation of the organisation will also affect its credit and market risk. A reputational event such as a serious hacking incident could therefore tarnish the reputation of an organisation (Vallens, 2008:43).

Credit and market risk can also be affected directly by IT risk. Sophisticated credit and market rating systems are dependent on IT for their operation. Any disruption in this regard, including an attack by hackers, could affect the availability of the credit and market rating systems or introduce data control weaknesses. The passing of unauthorised transactions, due to application control weaknesses, should also be considered as a possibility. These issues were identified as IT risks in section 4.3.5.17. Therefore, credit risk and market risk affect the control objectives authorisation, accuracy and integrity.

Thematological research questions

Based on the literature review above, the following thematological research questions can be defined:

Business risk
• The extent to which there is recognition of the existence of the link between hacking, IT risk and credit and market risk in the banking sector.
• The extent to which there is the possibility of a hacker incident that will affect the market and credit risk of the banking sector.
4.11 THE LINK BETWEEN HACKING, IT RISK AND COMPLIANCE RISK

As per the conclusion in section 4.3.10, compliance risk is related to an organisation’s ability to comply with applicable laws and regulations. Failure to do so could lead to fines, shutting down of business operations or criminal prosecution.

The complexity of legislation increases compliance risk, as pointed out in section 4.3.10. A significant IT risk theme identified in section 4.3.5.17 is cybercrime, which includes hacking. There are many legal pitfalls and ambiguities associated with cybercrime laws, such as the controversy related to the development of hacking tools by ethical hackers in the UK and in Germany (to be discussed in chapter 6). In general, it is difficult to prosecute hackers due to their anonymous activity and elusive nature (Bernard, 2001:66). An additional problem is that there are few countries that have no legislation available to prosecute hackers (Elms, LaPrade & Maurer, 2008:4). Hackers will seek out these countries, such as Yemen and North Korea, and route their attacks through these in order to avoid prosecution (Archick, 2006:CRS-3). The cross-border nature of hacking implies that various countries’ legislation will have to be considered, as pointed out in section 3.5.3.1. Although international organisations such as the United Nations (hereafter UN) and European Union (hereafter EU), through their directives, encourage international co-operation between member countries (Information Security Forum, hereafter ISF, 2005:14, 15), it remains questionable whether administrative arrangements will be effective enough to ensure successful cross-border prosecution of hackers, as discussed in section 3.5.3.1.

The very nature of the IT risk lack of compliance with IT policies, procedures, legal and regulatory requirements means that hackers will inevitably bring it into play. Hackers may completely ignore any legal or regulatory requirement, as discussed in section 3.5.2. As discussed in section 3.12.6, disclosure of data breaches is required by legislation in countries such as the US and Australia. When confidential client data is stolen through hacker activity, due to data control weaknesses, this could be interpreted as non-compliance with statutory requirements (Burris, 2008:28) and can even lead to penalties. This increases the organisation’s compliance risk. There is no doubt, of course, that organisations will have some form of insurance in place to cover such incidents, although this may come at a cost (Knapp & Boulton, 2006:83).

As per the first definition of compliance risk in section 4.3.10, organisations might make use of policies to ensure that employees comply with the relevant legislation. The threat posed by insiders is also applicable to the IT risk of non-compliance with IT policies and
procedures, as discussed in section 3.5.3.6. Therefore, non-compliance by insiders to legislation and specific policies (which can include IT policies) can also increase the compliance risk of an organisation.

The IT risk theme inadequate change and project management practices could also increase an organisation’s compliance risk, as in the example cited in section 4.3.10, where systems are not updated in time to comply with legislation and hacker breaches expose the non-compliance. The control objectives authorisation and confidentiality are affected by compliance risk.

<table>
<thead>
<tr>
<th>Thematological research questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Based on the literature review above, the following thematological research questions can be defined:</td>
</tr>
<tr>
<td><strong>Business risk</strong></td>
</tr>
<tr>
<td>• The extent to which there is recognition in the banking sector of the existence of the link between hacking, IT risk and compliance risk.</td>
</tr>
<tr>
<td>• Whether the banking sector has considered the most relevant IT risk, which may be exploited by hackers and increase the bank sector’s compliance risk.</td>
</tr>
</tbody>
</table>

### 4.12 THE LINK BETWEEN HACKING, IT RISK AND REPUTATIONAL RISK

As discussed in section 4.3.11, reputational risk can be defined as the change of shareholder, customer or public confidence or perception of an organisation, which could result in a sharp decline of the share price value, legal action or financial losses.

An IT security breach, as a result of a hacker event, could have a devastating impact on an organisation’s reputation, as was discussed in section 4.3.11. The impact could be exacerbated by the press, should it publish the incident. This could lead to loss of confidence from investors, clients and the general public. Ultimately this could seriously affect the financial performance of an organisation (Abbott, 2007).

Vulnerabilities in websites and web-applications could lead to website defacement, as discussed in section 3.9.3. Companies fear the reputational risk which may result from hacking incidents of this nature. Hacker attack types, such as DoS and web defacements, which damage the image of an organisation, could cause embarrassment for an organisation and affect its reputation. In fact, many of the activities of hackers could increase the reputational risk of an organisation, such as hacktivism (section 3.5.3.2) and cybercrime.
activities (section 3.10). These activities all give rise to some form of IT risk.

An Internet user invests an element of trust in an online organisation. If the user’s information has been compromised, it will affect the organisation’s reputational risk (Bornman, 2004:102). Whenever the organisation is dealing with confidential client data, such as in the case of Internet banking applications (pointed out in section 4.3.5.3 and 4.3.5.15.1), an IT risk, such as unauthorised logical access, could significantly increase the reputational risk of the organisation. In particular, when it becomes public knowledge that the client’s data has been compromised, the reputation of the organisation will be affected.

Ultimately, there is a close link between reputational risk, hacking and all the other business risk types discussed in section 4.3. The organisation will suffer reputational damage when the media reports on the following examples of business risks:

- **Physical risk**: Hackers breaching physical access controls, leading to theft of confidential client data.
- **Operational risk**: Operational business processes disrupted due to a security breach.
- **Human resource risk**: Employees inside the organisation, using hacking techniques to commit fraud or steal data.
- **Technology risk**: Outdated systems contain vulnerabilities, exploited by hackers.
- **Business continuity and disaster recovery**: DoS attacks severely disrupting business processes.
- **Credit and market risk**: Data integrity compromised due to successful hacker attacks, leading to the disclosure of inaccurate information to the market and lenders.
- **Compliance risk**: The organisation failing to comply with data privacy legislation, creating the impression that the organisation is negligent in securing confidential client data.

By implication, all IT risk themes and all the control objectives identified in this chapter may be affected. Reputational risk is therefore a significant contributor to business risk, with hackers playing a big part in blemishing the reputation of an organisation.

<table>
<thead>
<tr>
<th>Thematological research questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Based on the literature review above, the following thematological research questions can be defined:</td>
</tr>
<tr>
<td><strong>Business risk</strong></td>
</tr>
<tr>
<td>• The extent to which there is recognition in the banking sector of the existence of the link between hacking, IT risk and reputational risk.</td>
</tr>
</tbody>
</table>
• Whether the banking sector has considered the business risks which may be affected by reputational risk, as a result of successful hacker attacks.

4.13 CHAPTER SUMMARY

Chapter 3 established that hacking can be classified either as an event that results from a risk or risks, or as a risk per se. In this chapter, the link between (business) risk and hacking was explored further, based on the premise that an organisation’s responsibilities in addressing risk starts with a clear understanding of business risk.

Firstly, in this chapter it was established that there is no generic definition for business risk. It was further established that there is no generic classification of the categories of business risk. But the comprehensive literature review presented in this chapter has provided evidence that the risk categories in King II provide (and supported in principle by King III) an appropriate basis for the discussion of business risk. In addition, reputational risk has been added due to the importance of an organisation’s reputation. These resulting risk categories are:

- Physical risk.
- Operational risk.
- Human resource risk.
- Technology risk.
- Business continuity risk.
- Disaster recovery risk.
- Credit risk.
- Market risk.
- Compliance risk.
- Reputational risk.

Consequently, each of these risk categories was discussed in order to reflect on the meaning and scope of each. The discussion reflected further on the fact that there is overlap present between many of the risk categories. For example, the operational risk category relating to systems is closely linked to technology risk and IT.

As regards the risk category that received most attention, technology risk, the important focus on IT within technology risk was discussed in detail, as IT can be viewed in a number of ways, depending on the source or discipline. But this discussion has revealed that there
are a number of common IT risks or control objectives that are prevalent across most sources (presented in Tables 4.30 and 4.31).

Table 4.30  Common IT risks identified in the literature review (own summary)

<table>
<thead>
<tr>
<th>General controls:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Unauthorised physical access / lack of physical access control and security.</td>
</tr>
<tr>
<td>• Lack of compliance with IT policies and procedures, legal and regulatory</td>
</tr>
<tr>
<td>requirements.</td>
</tr>
<tr>
<td>• Business and IT disruption.</td>
</tr>
<tr>
<td>• Inadequate IT operations and support.</td>
</tr>
<tr>
<td>• Theft or damage to IT equipment.</td>
</tr>
<tr>
<td>• Inadequate change / project management practices.</td>
</tr>
<tr>
<td>• Misuse of IT / irregularities and fraud.</td>
</tr>
<tr>
<td>• Cybercrime.</td>
</tr>
<tr>
<td>• Unauthorised logical access.</td>
</tr>
<tr>
<td>• Inadequate IT performance.</td>
</tr>
<tr>
<td>• Complexity of IT.</td>
</tr>
<tr>
<td>• Inefficient use of IT resources.</td>
</tr>
<tr>
<td>• IT human resource deficiencies.</td>
</tr>
<tr>
<td>Application controls:</td>
</tr>
<tr>
<td>• Application control weaknesses.</td>
</tr>
<tr>
<td>• Data control weaknesses.</td>
</tr>
<tr>
<td>• Interface control weaknesses.</td>
</tr>
<tr>
<td>• Operating system weaknesses.</td>
</tr>
<tr>
<td>• Lack of an audit trail.</td>
</tr>
<tr>
<td>• Lack of segregation of duties.</td>
</tr>
</tbody>
</table>

Table 4.31  Common control objectives identified in this thesis (own summary)

<table>
<thead>
<tr>
<th>Control objectives:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Confidentiality</td>
</tr>
<tr>
<td>• Integrity</td>
</tr>
<tr>
<td>• Availability</td>
</tr>
<tr>
<td>• Accuracy</td>
</tr>
<tr>
<td>• Completeness</td>
</tr>
<tr>
<td>• Validity</td>
</tr>
<tr>
<td>• Security</td>
</tr>
<tr>
<td>• Authorisation</td>
</tr>
</tbody>
</table>

The common IT risks are used in the discussions to indicate the various links between IT risk, business risk types and hacking. Similarly, the control objectives either indicate what the characteristics are that the controls intend to achieve, or the opposite as a risk characteristic. Business risks, including IT risk and, by implication, hacking, could all threaten the achievement of these control objectives. Both the common IT risks and control objectives will be used as a basis in the remainder of this thesis.

Although there is such a close alignment between hacking and IT risk due to the pervasive impact of IT on business today, hacking incidents can also occur throughout an organisation and may be closely linked to each of the identified risk categories. As regards the close relationship between hacking, IT risk and the other categories, this chapter provides a discussion of the relationship between the three aspects. Indeed, all of the identified
categories of business risk may be adversely affected by hacking, either directly, or indirectly through the effect that hacking may have on the reputation of an organisation. The relationship between the categories of business risk, the identified IT risk themes or control objectives and examples of hacking is presented in Table 4.32.

The pervasiveness and intrusiveness of hacking in a range of business risk categories, which includes IT risk as a significant contributor to hacking events, have been presented. Hacking could potentially affect every IT risk theme and every control objective.

Table 4.32  Summary of the linkage between business risk, IT risk and hacking (own summary)

<table>
<thead>
<tr>
<th>Business Risk</th>
<th>IT risk themes with control objectives in brackets</th>
<th>Hacking Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical risk</td>
<td>• Unauthorised <em>(authorisation, security)</em> physical access, and lack of physical access control and security.</td>
<td>• Social engineering.</td>
</tr>
<tr>
<td></td>
<td>• Theft or damage to IT equipment <em>(security)</em>.</td>
<td>• Dumpster diving.</td>
</tr>
<tr>
<td></td>
<td>• Data control weaknesses <em>(confidentiality, integrity)</em>.</td>
<td>• Physical break-in and damage.</td>
</tr>
<tr>
<td></td>
<td>• Business and IT disruption <em>(availability)</em>.</td>
<td>• Theft.</td>
</tr>
<tr>
<td></td>
<td>• Social engineering.</td>
<td>• Key loggers / Sniffers.</td>
</tr>
<tr>
<td></td>
<td>• Dumpster diving.</td>
<td>• Backdoors / Trojans.</td>
</tr>
<tr>
<td></td>
<td>• Physical break-in and damage.</td>
<td>• Shoulder surfing.</td>
</tr>
<tr>
<td></td>
<td>• Theft.</td>
<td>• Wardriving.</td>
</tr>
<tr>
<td></td>
<td>• Key loggers / Sniffers.</td>
<td>• Social engineering.</td>
</tr>
<tr>
<td></td>
<td>• Backdoors.</td>
<td>• Shoulder surfing.</td>
</tr>
<tr>
<td></td>
<td>• Shoulder surfing.</td>
<td>• Collaboration with insider.</td>
</tr>
<tr>
<td></td>
<td>• Wardriving.</td>
<td>• Privilege escalation.</td>
</tr>
<tr>
<td></td>
<td>• Data theft.</td>
<td>• Data theft.</td>
</tr>
<tr>
<td>Operational risk</td>
<td>All IT risk themes and control objectives are relevant.</td>
<td>All hacking attack types are relevant (refer to section 3.9 for attack types and 3.13 for the effect of hacking on business).</td>
</tr>
<tr>
<td>Human resource risk</td>
<td>• Lack of compliance with IT policies and procedures <em>(validity)</em>.</td>
<td>• Backdoors.</td>
</tr>
<tr>
<td></td>
<td>• Business and IT disruption <em>(availability)</em>.</td>
<td>• Social engineering.</td>
</tr>
<tr>
<td></td>
<td>• Poor project management practices.</td>
<td>• Shoulder surfing.</td>
</tr>
<tr>
<td></td>
<td>• Misuse of IT / irregularities and fraud <em>(integrity, validity)</em>.</td>
<td>• Collaboration with insider.</td>
</tr>
<tr>
<td></td>
<td>• Unauthorised logical access <em>(security)</em>.</td>
<td>• Privilege escalation.</td>
</tr>
<tr>
<td></td>
<td>• Lack of segregation of duties <em>(authorisation)</em>.</td>
<td>• Data theft.</td>
</tr>
<tr>
<td></td>
<td>• Human resource deficiencies <em>(accuracy)</em>.</td>
<td>• Social engineering.</td>
</tr>
<tr>
<td></td>
<td>• Complexity of IT <em>(accuracy)</em>.</td>
<td>• Shoulder surfing.</td>
</tr>
<tr>
<td>Technology risk</td>
<td>All IT risk themes and control objectives are relevant.</td>
<td>All hacking attack types are relevant.</td>
</tr>
<tr>
<td>Business continuity and disaster recovery</td>
<td>Business and IT disruption <em>(availability)</em>.</td>
<td>• DoS.</td>
</tr>
<tr>
<td></td>
<td>• Application control weaknesses <em>(accuracy, integrity)</em>.</td>
<td>• Malware.</td>
</tr>
<tr>
<td></td>
<td>• Data control weaknesses <em>(authorisation, integrity)</em>.</td>
<td>• Web-defacement.</td>
</tr>
<tr>
<td>Compliance risk</td>
<td>• Lack of compliance with IT policies and procedures, legal and regulatory requirements.</td>
<td>• Physical damage.</td>
</tr>
<tr>
<td></td>
<td>• Hackers show a total disregard local and international legislation (and supporting policies).</td>
<td>• Alteration of data and programmes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Theft of data and programmes.</td>
</tr>
<tr>
<td>Business Risk</td>
<td>IT risk themes with control objectives in brackets</td>
<td>Hacking Examples</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>• Data control weaknesses (authorisation, confidentiality).</td>
<td>• Security breaches.</td>
</tr>
<tr>
<td></td>
<td>• Complexity of legislation.</td>
<td>• Identity theft.</td>
</tr>
<tr>
<td></td>
<td>Most IT risk themes (and control objectives), when disclosed to regulators and stakeholders.</td>
<td>• Phishing.</td>
</tr>
<tr>
<td>Reputational risk</td>
<td></td>
<td>• DoS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Web-defacement.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• All attack types, when disclosed.</td>
</tr>
</tbody>
</table>

This chapter has also shown the reputational risk organisations carry when they are unable to protect themselves against the significant threat of hacking. Therefore, attention must turn to the range of responses available to address the risk of hacking, which is the subject of chapter 5.
CHAPTER 5
The responses to hacking

5.1 INTRODUCTION

The pervasive and intrusive nature of hacking as a threat to many organisations is evident from the discussion in previous chapters. In chapter 3, it was established that hacking is an event that results from a risk or risks and that hacking can indeed be classified as a risk. It has further been established that there is a close link between hacking and business risk. Each of the risk categories identified in King II and supported by risk management principles defined in King III can be adversely affected by hacking. Therefore a response is needed. An extensive literature review has revealed that there is no single solution that can be employed to address the risk of hacking.

Therefore, this chapter will firstly categorise the broad responses to hacking to facilitate the discussion. The range of responses includes corporate governance, risk management, internal control, IT governance, service management, quality management and software development, and lastly information security management. Each discussion will provide the necessary context and application of the response. The discussion of each response will also include insight into the common best practice frameworks, dimensions, role-players, advantages and disadvantages. This is further supplemented by linking the response to the IT risk themes identified in this thesis. This will provide a view on the effectiveness of each response in addressing the pervasive nature of hacking, due to its strong association with IT risk and highlight that that some responses are more effective in addressing the hacking threat than others. The chapter concludes by arguing that a more effective response to hacking is required. This will lead into chapter 6, where ethical hacking as a comprehensive response to hacking will be discussed.

5.2 IDENTIFYING AND CATEGORISING THE VARIOUS RESPONSES TO HACKING

To mitigate the risks and events emanating from hacking, a response is required. A host of responses to the threat of hacking are available to organisations. These responses may vary from a general approach to the threat of hacking that implies that it receives no more
attention than any other risk, to detailed technology solutions when the threat is deemed to be pervasive to the extent that an event or risk can cripple an organisation. Ideally, the response should be a direct response and effective enough to prevent or mitigate the risk. The response would also be considered a direct response when it addresses the IT risk themes identified in this thesis, since it has been demonstrated in section 4.4.1 how closely hacking can be associated with each IT risk. It should also be recognised that the responses considered in this section have varying dimensions. A particular response might provide a high level, process level or a deep technical response to IT risks and hacking. The responses could also be direct or indirect in nature to IT risks and hacking. It could also focus on the risk or event component of hacking, as presented in Figure 3.3, followed by the preventative or detective nature of the response, as established in section 4.3.5.11.

Since corporate governance can be regarded as an overarching response, the responses to IT risk from a corporate governance perspective will be briefly considered. Both King II and King III require the board of directors to take responsibility for the organisation’s risks. The first response to organisational risks from a King II and King III perspective is risk management (IoD, 2002:86; IoD, 2009b:31, 73). As a further response, the board of directors needs to ensure that an effective system of internal control has been imbedded in the organisation (IoD, 2002:82; IoD, 2009b:31, 95). The board of directors is also responsible for selecting the most appropriate risk management and internal control frameworks (IoD, 2002:30). King III recognises the significance of IT risk in an organisation and recommends IT governance as a response (IoD, 2009b:31, 82). Therefore, the first four broad response categories to consider are: corporate governance, risk management, internal control and IT governance.

Many frameworks, standards or tools have been developed to assist with the implementation of the four responses identified in the preceding paragraph. Due to the diverse nature of the various frameworks, standards or tools, a further extension of the four response categories might be required. It would therefore be useful for the discussion in this chapter to identify an extension or reduction to the four categories already identified, to facilitate a more logical grouping of similar responses.

Although extensive literature exists which discusses various corporate governance and IT governance frameworks and standards in general, such as Larsen, Pedersen & Andersen (2006:5), Eslami, Fasanghari & Abdollahi (2007:75-76), Wallace & Webber (2009:4-8), Calder (2008a) and Flowerday and Von Solms (2005) none of them proposes a logical grouping from a governance perspective. The Certified in the Governance of Enterprise IT
(hereafter CGEIT) training material proposes the following governance framework categories, presented in Table 5.1.

### Table 5.1 Governance framework categories (Pankey, 2010:4)

<table>
<thead>
<tr>
<th>Category</th>
<th>Type</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Governance</td>
<td>Focus on how to manage information, IT and communication technology efficiently and effectively.</td>
<td>CobiT, Val IT</td>
</tr>
<tr>
<td>Service Management</td>
<td>How to perform and organise IT management, such as service delivery and support.</td>
<td>ITIL, Generic Framework</td>
</tr>
<tr>
<td>Quality Management</td>
<td>Quality standards applied to IT domains.</td>
<td>ISO 9000, ISO 20000, ISO 27001</td>
</tr>
<tr>
<td>Quality Improvement</td>
<td>Improvement of processes or performance</td>
<td>IT BSC, CMMI, Six-Sigma</td>
</tr>
<tr>
<td>Project Management</td>
<td>Portfolio, program &amp; project management.</td>
<td>PMBOK, MSP, PRINCE2</td>
</tr>
<tr>
<td>Risk Management</td>
<td>Identifying &amp; managing risk.</td>
<td>RiskIT, OCTAVE, FIRM, AS/NZ 4360</td>
</tr>
</tbody>
</table>

When considering the table above and the four broad response categories identified earlier in this section, further response categories can be identified and similar categories can be combined to facilitate the discussion in this chapter. Quality management, quality improvement and project management categories will be combined, since they mostly provide an indirect response to the IT risks and hacking. Service management will remain a separate category, since it does not logically group with another category and also does not provide a direct response to IT risks and hacking. King III requires the risk committee and the audit committee to guide the board of directors in carrying out their IT responsibilities. As part of these responsibilities, the board of directors will have to demonstrate that it has considered information security management practices (Nkonki Inc. 2009:25).

Information security management will therefore be defined as an additional category to those already identified, due to the relevance and importance of information security management as a response to IT risk, cybercrime and hacking. ISO 27001 will be regrouped under this category, due to its strong association with information security management. Therefore, the resulting categories identified are: corporate governance, risk management, internal control, IT governance, quality management, service management and information security management. The first response category explored is the corporate governance response.
5.3 HACKING AND THE CORPORATE GOVERNANCE RESPONSE

5.3.1 The essence of the corporate governance response

It was established in section 2.1 that IT has a significant impact on corporate governance. Further, Tables 2.1 and 2.2 presented recommendations from King II and King III related to IT that emphasised that boards of directors need to ensure that the necessary skills are in place to ensure that their responsibilities in respect of internal control systems are adequately discharged, that technology benefits are embraced and that the risks associated with the blurring of organisational boundaries due to technology have been addressed. Section 4.3.5.5 expanded further on the importance of IT risk in King II and King III and commented on the emphasis in King II (and even more so in King III), that IT plays an important role in achieving risk based principles of validation, security, integrity, availability and continuity. As this thesis has provided clear evidence that hacking is closely linked to IT risk and to the other business risk categories identified in section 4.2.4, it is therefore appropriate to present corporate governance principles as the first response to hacking.

Broadly speaking, corporate governance emerged as a consequence of the separation of shareholders (owners) from the management of an organisation. The most visible consequence of this separation is the appointment of a board of directors (Rossouw, Prozesky, van Heerden & van Zyl, 2006:116). Briefly, a distinction must be made between broad and narrow corporate governance. The former refers to how companies are controlled from outside the organisations through regulation by state institutions and legislation, while the latter refers to governance from within and details that which is the responsibility of the board of directors (Rossouw, et al. 2006:124-125).

As the responses to hacking is organisation specific, in the context of this thesis, the corporate governance responses to hacking will fall in the category of narrow corporate governance, to which a host of different meanings may be attached. The Cadbury Report of 1992 defined it as “the system by which companies are directed and controlled” (Committee on the Financial Aspects of Corporate Governance and Gee and Co. Ltd. 1992:14). A similar definition was published by the OECD in 1999 (as quoted by Smerdon, 2007:1, 3):

Corporate governance is the system by which business corporations are directed and controlled. The corporate governance structure specifies the distribution of rights and responsibilities among different participants in the Corporation, such as the board, managers, shareholders and other stakeholders, and spells out the rules and procedures for making decisions on corporate affairs.
Given the focus on IT risk and hacking, Lam (2003:53) recognised the purpose of corporate governance as the mechanism to ensure that the “board of directors and management have established the appropriate organizational processes and corporate controls to measure and manage risk across the company”. Therefore, corporate governance and its resultant codes focus on the means to direct and control organisations, while managing the associated risk. Currently in South Africa, the relevant code that sets out how narrow corporate governance is to be achieved is King III, as already recorded. It also needs to be considered that King III has been issued due to changes in international governance trends since the release of King II and by implication reflects international best practice in corporate governance (IoD, 2009a:4; PwC, 2009b:1).

Of particular importance in the context of this thesis is the clear introduction of IT governance in King III. It recognises the significance and importance of IT in organisation’s today and the need to manage both the significant investment, but also the risks introduced by IT. An entire chapter in King III (chapter 5) is dedicated to the principles of IT governance. Organisations are required to formalise their IT governance practices, by implementing an IT governance framework (IoD, 2009b:16; Badenhorst, 2009:7; Scholtz, 2010:1). In addition, there are several complementary corporate governance responses to hacking defined by King II and King III. It will be shown in this section that the focus is primarily on managing risk, establishing internal controls and implementing effective IT governance processes.

Foremost is the principle that the board of directors is responsible for corporate governance, towards ensuring effective control of the organisation (IoD, 2002:21; IoD, 2009b:20). This implies that the board of directors is responsible for defining appropriate responses to hacking. The board of directors is in particular responsible for identifying key risks that may be detrimental to the survival of the organisation (IoD, 2002:22; IoD, 2009b:29) or threaten the income streams, critical business processes or even stakeholder expectations (IoD, 2009b:77). It has already been established in section 4.2 of this thesis that there are key business risks organisations need to manage and monitor. These key risks should form part of the organisation’s register of key risks (IoD, 2002:32; IoD, 2009b:77). In the conclusion of chapter 4, the pervasive nature of hacking across business is highlighted and how it could increase each of the key business risks discussed throughout chapter 4. It also emphasises the need to include the risk of hacking into the organisation’s register of key risks, if it is applicable to the size and complexity of the organisation, and the risk tolerance levels the organisation is willing to accept.

The internal governance issues an organisation face include attaining thorough knowledge
of IT processes and technology, while treating information as an organisational resource (ITGI, 2005a:27). Coupled with this is the responsibility to identify the risks which threaten an organisation’s information assets. The board of directors is ultimately responsible for risk management system (Du Plessis, McConvill and Bagaric, 2005:56) towards mitigation of the information security risks. The board of directors’ responsibility for identifying key risks is further entrenched in the following principle (IoD, 2009b:77): “Principle 4.6: The board should ensure that frameworks and methodologies are implemented to increase the probability of anticipating unpredictable risks”. Given the covert nature of hacking activities (as discussed in sections 3.3.3, 3.9.1.1, 3.11.3.1 and 3.13), it might be challenging to mitigate the risk of hacking. Of course, the board of directors may delegate this responsibility to management (IoD, 2002:79; IoD, 2009b:78). The board of directors is however ultimately responsible for defining risk tolerance levels (IoD, 2002:78; IoD, 2009b:74). In response to the unpredictable nature of risk, the board of directors may need to establish a risk management function (IoD, 2002:77; IoD, 2009b:75) which can be used as a response to the risk of hacking. The board of directors is also responsible for establishing IT governance, including an IT governance framework which ultimately addresses significant IT risks (IoD, 2009b:82), such as the risk of hacking.

The board of directors is also responsible for reporting on the effectiveness of the organisation’s internal controls (IoD, 2009b:31). Internal controls are established in an organisation to mitigate the business and IT risks (Wixley & Everingham, 2010:90), which may include the risk of hacking.

5.3.2 Application of the corporate governance response

The corporate governance response to hacking serves as an overarching response, which binds the other responses to hacking together and places the responsibility of the various responses in the remit of the board of directors. King III has adopted an “apply or explain” approach towards following corporate governance principles. It requires organisations to consider the applicability of the corporate governance principles set out by King III (IoD, 2009b:7). Organisations are encouraged to select the principles which are appropriate to their size, nature and complexity (PwC, 2010a:2, 3). Organisations would therefore follow the principles that are applicable, rather than being burdened with corporate governance principles which are not appropriate for the type or size of organisation in question. Organisations can also respond to IT risk through the formation of a technology committee, specifically tasked with addressing IT and technology issues. The board of directors may delegate IT issues to this committee, which consists of members with the required
knowledge to evaluate the organisation's technology strategy (Premuroso & Bhattacharya, 2007:1260, 1261, 1263). This committee could also be responsible for reviewing of significant IT risks, such as hacking.

As already discussed, corporate governance encourages the establishment of risk management, internal control and IT governance practices. Arguably though, organisations of any size or type should, at a minimum, follow risk management and internal control practices. At their most basic level, these could provide a response to IT risk, including the risk of hacking.

5.3.3 Dimensions of the corporate governance response

Corporate governance is a high-level, overarching response and does not provide detailed process steps or technical guidance for the mitigation of IT risks, including hacking. Corporate governance addresses both the risk and event components of hacking. It is submitted that risk is encountered in all facets of business. King II articulates it as follows: “enterprise is the undertaking of risk for reward” (IoD, 2002:76). Strategy in itself involves risk, because an organisation is dealing with uncertain future events (or risk) (IoD, 2002:76; IoD, 2009b:15, 118). From an event perspective, King III recognises that an event “can be a single occurrence or a series of occurrences” (IoD, 2009b:123). King III also considers the effect of external events (IoD, 2009b:101) and security events (IoD, 2009b:121). Therefore, in the context of South African corporate governance codes, hacking should be managed from a risk and event perspective.

Following on from the risk and event perspective is the question of whether corporate governance recognises the preventative and detective nature of controls. King III makes several references to the concept “prevent” (IoD, 2009b:9, 10, 26, 37, 73, 80, 94, 96, 101, 102, 119, 120). From a detective perspective, King III makes only one reference to the concept “detection” (IoD, 2009b:121). It is submitted that a word often used in the same context as detection, “monitoring”, can also be used to test whether either King II or King III refers to the detective nature of controls. Monitoring of risks is a fundamental principle highlighted in King II (IoD, 2002:83, 237, 238). The words “monitor” and “monitoring” are used numerous times in King III (IoD, 2009b:26, 29, 33, 34, 35, 37, 49, 59, 62, 65, 66, 74, 75, 76, 79, 84, 85, 86, 87, 89, 90, 114, 115, 121, 124, 125, 126, 127). Since there is such a significant emphasis on the concept “monitoring”, it can be inferred that King II and King III, and consequently corporate governance, focus on both the preventative and detective nature of controls.
5.3.4 Role-players in the corporate governance response

There are various role-players involved from a corporate governance perspective. Accountability starts with the uppermost body in the organisation, the board of directors. King II and King III place the responsibility of corporate governance on the shoulders of the board of directors (IoD, 2009b:29). The board of directors should have a common understanding of the day-to-day business of the organisation and the pertinent issues faced by the organisation (Du Plessis, et al. 2005:57), such as the threat posed by hackers. The board of directors is also responsible for approving the internal control and risk management system (Du Plessis, et al. 2005:56), towards the prevention and detection of the hacker threat.

Advancement in IT is enabling prospective investor and shareholder access to information about an organisation's performance, which might not have been available in the past. IT bring with it increased and complex risks, which may affect the bottom-line. The board of directors will increasingly be held accountable for their investment decisions in IT and greater transparency is required by shareholders (Chau, 2011:11-12). The risk of hacking has been identified in this thesis as a significant IT risk. It is therefore an important consideration to determine how the board of directors responds to and discloses IT risk.

As a requirement of corporate governance, risk management is often embedded in the day-to-day operations of an organisation. Every employee is therefore responsible for risk management (IoD, 2002:77; IoD, 2009b:75), but the overall responsibility for risk management still rests with the board of directors (IoD, 2002:79). This responsibility could be delegated to a risk committee (or audit committee) who should provide the necessary oversight and policy guidance (IoD, 2002:79; IoD, 2009b:75). Regardless, the audit committee plays a role in the organisation's risk management process (Davies, 2009:44; IoD, 2009b:63). In particular, the audit committee should ensure that IT risks, as it relates to financial reporting have been addressed (Hadden & Hermanson, 2003:38; IoD, 2009b:64). The board of directors and the audit committee should pay attention to significant IT risks, which may include hacking. The audit committee provides oversight over the internal audit function, ensuring that it is independent and in a position to discharge its assurance role (IoD, 2002:137; IoD, 2009b:63). The internal audit function is responsible for providing assurance that significant risks, which may prevent the achievement of strategic goals, are appropriately mitigated through internal controls (IoD, 2002:94; IoD, 2009b:94). Internal audit therefore also plays a role in providing assurance that internal controls are in place to mitigate the risk of hacking. Internal control could be in the form of a process response, such
as risk management or IT governance, or could be operational in nature, such as technical controls.

5.3.5 Advantages of the corporate governance response

Corporate governance ensures that the board of directors is held accountable for the risk management and internal control processes. The strong emphasis of corporate governance on risk management ensures that significant business and IT risks are identified, managed and mitigated.

A study focusing on corporate governance trends has highlighted that organisations that have adopted corporate governance codes (such as the Cadbury Report in the UK) have shown increased financial performance (McKnight, Milonas, Travlos & Weir, 2009:40). A similar study has shown that the formation of a technology committee contributes to the profitability of an organisation and increases the organisation’s shares performance. The study included a review of the board sub-committees of organisations listed on the Standards & Poor 500 during 2006, with 23 organisations identified as having a technology committee at board level (Premuroso & Bhattacharya, 2007:1273, 1265). The formation of a technology committee strengthens the corporate governance processes of the organisation and ensures IT issues and risks receive attention, while creating shareholder value.

Following corporate governance principles will ensure that the board of directors establishes the business direction for the organisation, to ensure that strategic objectives are achieved. In addition, it will also instil the required supervision and control (Rossouw, et al. 2006:116-117), such as ensuring compliance with external regulations, while gaining “competitive advantage through improved control” (Handley-Schachler, Juleff & Paton, 2007:630). Internal control, in turn, could be defined to address IT risks.

Good corporate governance facilitates the formulation of a good business strategy, due to the participation of non-executive directors or external board members, who could provide a fresh perspective on the organisation’s business objectives. Effective corporate governance also attracts much-needed funding from investors and financial institutions. These benefits do not apply to large organisations only, but can also be beneficial to small to medium-sized organisations (Abor & Adjasi, 2007:117-118). Over and above attracting investor capital, the board members also bring much needed intellectual and reputational capital to the organisation, which could increase the performance of the organisation. The ethical values displayed by board members could also increase employee motivation, which also may lead
to increased performance (Gill, Vijay & Jha, 2009:9). It is submitted that non-executive directors or external board members could also provide insight into the mitigation of IT risks.

Using corporate governance as a response to IT risk themes, including hacking, ensures that the board of directors and other senior stakeholders are aware of the risks associated with hacking, as well as the mitigating responses in place to address the threat. It is submitted that the benefit of having senior stakeholders involved in mitigating the threat of hacking is that it may lead to a more agile response from a governance perspective in general. Then not only may the direct responses to the hacking threat be more effective, but supporting processes may also be more effective, such as change, incident and business continuity processes. A further benefit is the allocation of funding to initiatives which would address hacking events or mitigate hacking risks. The response to hacking will also be integrated with other corporate governance processes, such as risk management. It is also possible that the board of directors would seek assurance from the audit committee as to whether the risk of hacking has been adequately addressed. This facilitates a layered and integrated response to the threat of hacking.

5.3.6 Disadvantages of the corporate governance response

The high cost of effective corporate governance is a decisive factor in defining it as an effective response (Abor & Adjasi, 2007:118). Implementing corporate governance will require audit personnel, additional committees and more directors, at higher salaries due to their increased responsibility (Abor & Adjasi, 2007:118). Although larger organisations might be able to carry the cost associated with corporate governance, smaller organisations might find it difficult to implement a comprehensive system of corporate governance (Aguilera, Filatotchev, Gospel & Jackson, 2007:14). The cost factor therefore might be a determining factor in defining and implementing a response to the hacking threat.

Corporate governance in itself is not a direct response to the hacking threat. It will have to be augmented by other responses. Nor does it provide a detailed response to IT risks or hacking. King III encourage the use of best practice frameworks towards the implementation of IT governance and risk management practices (IoD, 2009b:16, 74), which provides operational guidelines, not necessarily defined in King III.
5.3.7 Risks addressed by the corporate governance response

Corporate governance and the corresponding South African codes, King II and King III, do not address IT risks or hacking directly. But, the King II business risks formed the foundation for the business risks identified in this thesis. In addition, the focus on risk management by both King II and King III highlights that corporate governance will identify significant business risks (which includes IT risk) in general, although at a higher level. Detailed risks, similar to the IT risk themes are not identified by corporate governance codes. However, when supplemented by other frameworks, detailed risks might be addressed through the application of corporate governance principles.

From a control objectives perspective (as identified in Table 4.26), King II makes general references to control objectives, such as integrity, accuracy and authorisation (IoD, 2002:28, 83, 148). Specific reference is made to “validation, security, integrity, availability and continuity” from a technology and IT perspective (IoD, 2002:84). King III refers to the information security principles, confidentiality, integrity and availability (IoD, 2009b:87). Several general references are made to other control objectives, such as accuracy, completeness and security (IoD, 2009b:108, 110, 124). Therefore, from a corporate governance perspective, all the control objectives are considered.

5.3.8 Conclusion

From a corporate governance perspective, the board of directors remains responsible for identifying key business risk. Within that process, the board must ensure that business risk is addressed on a continuous and systematic basis, through appropriate frameworks and methodologies. Corporate governance is in itself not a direct response to the threat of hacking and has to be augmented by other responses or frameworks to ensure a more direct response. However, corporate governance as a response remains important, since it binds other responses and provides a direct link and accountability with the board of directors.

What needs to be acknowledged is that risk management and a system of internal control will be necessary to prevent and detect risk. It is ultimately up to the board of directors to determine whether technology or IT, and specifically hacking, is a significant actual and/or potential risk to the organisation, and within this process it is important that the board of directors formulates a determination on its appetite or tolerance for risk. Lastly, it must be acknowledged that there are a range of parties that will be involved in this process.
Thematological research questions

Based on the literature review above, the following thematological research questions can be defined:

Hacking response
- The extent to which the banking sector will rank corporate governance as an effective response to hacking.
- The extent to which the awareness of hacking at a board of directors' level may lead to a more effective response to the threat of hacking in the banking sector.
- The extent to which certain aspects of technology or IT risk, such as the risk of hacking, is identified as a matter for specific attention either through the risk management process, IT governance or through internal controls in the banking sector.
- The extent to which there is recognition in the banking sector that attention must be paid to risk management, IT governance, as well as internal control systems, as part of the corporate governance response to the risk of hacking.
- The extent to which the banking sector has made use of a technology committee, to address IT-related issues and risks.
- The extent to which the banking sector makes use of a technology committee to address the threat of hacking.
- Whether there is recognition that an agile corporate governance process will ensure an effective response to the threat of hacking in the banking sector.

Business risk
- The extent to which technology or IT risk is recognised as a key business risk at board level in the banking sector.
- The extent to which there is a determination of the risk tolerance or risk appetite for hacking in the banking sector.
- The extent to which there is recognition at board level that hacking is a risk that needs specific attention.

IT risk
- The extent to which hacking has been considered as a technology or IT risk in the banking sector.
- Establishing who is responsible for identifying aspects of IT risk that need to be addressed specifically, within the banking sector.

5.4 HACKING AND THE RISK MANAGEMENT RESPONSE

5.4.1 The essence of the risk management response

The importance of risk management as a response has been highlighted under the umbrella of the corporate governance response. Organisations of all types and sizes have a need to identify and assess their risks, towards achievement of their organisational goals (AIRMIC, ALARM & IRM, 2010:2). Therefore, the second response to hacking is to address it as part of the risk management process.

Risk management plays a significant role from a corporate governance perspective. The
The board of directors is responsible for the governance of risk (IoD, 2009b:73), which may include the key risk area of hacking at the detailed level, or the key risk area of IT risk at a higher level. Risk management can be defined as management’s action towards controlling the organisation’s risk. The objective of risk management is to ensure risks are “maintained at an acceptable level” (NIST, 2000, as quoted by Kritzinger, 2006:73). Risk management involves a continuous process that includes steps such as risk identification, risk evaluation, risk monitoring and risk reporting. The risk management process is also accompanied by a risk management strategy or policy to ensure adherence and embedment in the organisation (Valsamakis, Vivian & du Toit, 1999:25; Olsson, 2002:107; Merna & Al-Thani, 2005:50-51). As already discussed, the risk committee is responsible for setting the risk management policy and linking it back into the organisation’s corporate governance responsibilities.

The risk management plan or process should be based on best practice risk management and ERM frameworks, such as COSO; ISO 31000:2009; Institute of Risk Management South Africa (hereafter IRMSA) ERM Code of Practice; or Institute of Risk Management United Kingdom (hereafter IRM (UK)) Risk Management Standards (IoD, 2009b:74). Examples of basic risk management frameworks (ISO 31000:2009, AIRMIC, ALARM & IRM Risk Management Standard and NIST Special Publication 800-30 (hereafter NIST SP 800-30)) will be briefly discussed:

- ISO 31000:2009 is an international standard for the implementation of risk management principles and only provides generic guidelines for the design and implementation of a risk management process (AIRMIC, et al. 2010:3, 7; International Organization for Standardization, hereafter ISO, 2010a). The ISO risk management process includes two key steps in its iterative process: risk assessment and risk treatment (AIRMIC, et al. 2010:7). Risk assessment involves the process of identifying the risk within the context within which an organisation operates. Risk treatment involves the process of identifying and implementing control measures to mitigate or modify the identified risk (AIRMIC, et al. 2010:8; Purdy, 2010:884).


- NIST SP 800-30 “Risk Management for Information Technology Systems”, is a unique framework since it utilises ethical hacking techniques specifically towards the
identification of hacking risks. The framework includes nine risk assessment activities, including the activity “system characterisation”, which recommends the use of automated scanning tools. The threat identification activity could be used to identify hacker or insider activity. Ethical hacking in particular could be used during the vulnerability identification activity (Stoneburner, et al. 2002:15, 17).

What these risk management standards have in common is an attempt to formalise the risk management process, even though each might have a slightly different approach to implementing and operating a risk management process. Organisations also have a decision to make concerning the maturity level of the risk management process to be achieved. A risk maturity model, such as the Risk and Insurance Management Society (hereafter RIMS) model, could assist in this endeavour (Coetzee & Lubbe, 2011:5, 6, 8). An organisation will have to select the most appropriate framework for its risk environment.

Management are increasingly starting to implement IT risk management practices in their organisations, due to an increase in IT risk (Barnier & Westerman, 2009:3). Factors leading to the increase in IT risk include greater complexity in IT, an increase in the cost of IT incidents and the general need to lower cost, many of which were discussed in chapter 2. Pressure to comply with increasing regulatory requirements also increases IT risk (Barnier & Westerman, 2009:4). In order to address IT risk (including hacking) in a risk management process, a formal approach is necessary to unlock the advantages of the risk management process. Selecting a risk management framework will assist management in measuring, managing and reporting on IT risk (Rudman, 2008:12). Examples of IT risk management frameworks include OCTAVE, Factor Analysis of Information Risk (FAIR), NIST’s Risk Management Framework (RMF) and the Threat Agent Risk Assessment (TARA) (Violino, 2010). The identification of IT risk depends on the maturity of risk governance processes (Barnier & Westerman, 2009:6). This highlights the importance of the IT risk management discipline linking into the organisation’s risk management and corporate governance processes. The ultimate objective of IT risk management is to enhance the way an organisation manages its IT (Barnier & Westerman, 2009:10).

5.4.2 The Enterprise Risk Management (ERM) response

Although risk management has strong merits, it tends to be performed in a silo-based fashion. The need for a more integrated, organisation-wide risk management process has led to the development of ERM (Truter, 2007:4). The reason for following an ERM approach is evident from the following quote (Truter, 2007:5):
ERM is interrelated with corporate governance in that it provides the board with a comprehensive overview of the risks faced throughout the organisation and control measures implemented both to eliminate and to mitigate risk.

Due to the pervasive nature of IT in an organisation, IT risk could also occur across an entire organisation, increasing the business risk of an organisation, as explained in chapter 4. A risk management response is required to address both business and IT risk. ERM encapsulates this by monitoring and managing financial and non-financial risk across an organisation. Within an ERM approach, organisations manage risk as a portfolio that includes various business risks in an effort to identify threats and events that may have an impact on the organisation. This in turn leads to the management of risks within defined risk tolerance levels (Pickett, 2006:28). The tolerance levels must also be defined for the risk of hacking. ERM can be implemented through ERM frameworks, such as COSO ERM, and the IRMSA ERM Code of Practice. The COSO ERM framework can be used as a baseline or benchmark for internal control and risk management. It is widely cited as a best practice framework (Kinney, 2003:140; De la Rosa, 2006:11; Rezaee, 2007:522; Wixley & Everingham, 2010:90-91; Beasley, Branson & Hancock, 2010:iii, 2, 6). The COSO ERM framework recommends that management should define its risk appetite towards meeting the organisation’s strategic objectives. In addition, ERM should allow for appropriate risk decision-making, such as avoiding, reducing, sharing or accepting risks.

Organisations face various business risks. The COSO ERM framework suggests that the ERM solution should be able to respond to pervasive integrated risks. An ERM solution provides a consolidated view of all possible events, which would allow management to seek beneficial opportunities (COSO, 2004:1). ERM, as arguably best depicted in the COSO ERM framework, is therefore an effort to consolidate the various risks faced by an organisation, rather than following a silo-based approach to managing each risk. The consolidated approach ensures that the relationships between the various risks are identified and shared with all stakeholders (Walker, Shenkir & Barton, 2002:24-25).

The IRMSA ERM Code of Practice defines 10 principles of ERM, which include aspects such as making the board of directors responsible for ERM, establishing a framework for ERM, defining a process for ERM and embedding ERM within the organisation (IRMSA, 2007:16, 19, 26, 41). These frameworks recognise the importance of a consolidated response across the organisation and closer alignment with corporate governance.
5.4.3 Application of the risk management or ERM response

The risk management process, such as that contained in best practice risk management frameworks, could be used to identify the risk of hacking. Most organisations, irrespective of their size and complexity, are affected by a disparate range of risks. A risk management process would aid in the identification of significant risks (Louw, 2007:24, 44, 57). The risk of hacking can be considered both as an internally and externally driven risk. Internally, it is an operational risk (as discussed in section 4.6). Externally it could be identified as a threat to the continuity of the organisation (as discussed in section 4.9). The probability of occurrence needs to be determined for the risk of hacking, which may vary depending on the size, complexity and extent of IT automation in the organisation. Alternatively, it is possible that the risk management process would identify significant risks associated with the likelihood of hacking materialising, rather than the risk of hacking itself. This would include, for example, identifying insecure systems or a weakness in a process which ensures regular patch updating. An IT risk management process in particular could be used to identify the IT risk themes identified in this thesis, which are closely associated with the risk of hacking. Once the risks have been identified, this would lead to risk treatment or risk response. Responses to risks as part of a risk management process includes avoiding, mitigating, transferring, accepting, exploiting, terminating and integrating the risks (IoD, 2009b:78). Risk treatment could also involve the identification of appropriate controls, such as technical controls or ethical hacking (discussed in chapter 6). Controls should be measured against the control objectives, to ensure they achieve the desired management objectives.

The likelihood of hacking could also be assessed as part of the ERM process, as well as imbedding appropriate mitigation and monitoring processes towards the identification of the risk of hacking. One of the benefits of ERM, as opposed to a general risk management process, is that ERM identifies IT risk at a high level and also potentially the risk of hacking at a lower level, across the entire organisation. ERM takes a far more comprehensive view on risk in an organisation, and could also aid in identifying responses to the risk of hacking which could cover the entire control environment of an organisation.

5.4.4 Dimensions of the risk management or ERM response

Risk management and ERM provide guidance towards the management of organisational risk from a process perspective. The focus is on business risks that are significant to the business, identified via a systematic risk management process. Risk management and ERM take a forward-looking view towards possible unknown events in the future. Risk
Risk management and ERM frameworks include steps which lead to the identification of an appropriate response or controls to mitigate the risk identified. Deterrent countermeasures are often non-technology-based, whereas preventative countermeasures are often technology-based solutions, in particular those preventing information security incidents (Taylor, 2009:50). It follows that from a hacking risk perspective, the response or control will most likely be a technology-based solution and therefore preventative in nature. The risk management process as a response to the risk of hacking is therefore preventative in nature.

5.4.5 Role-players in the risk management or ERM response

From a corporate governance perspective, various role-players might be involved in the organisation’s risk management or ERM processes, such as the board of directors, the risk committee or audit committee, management and internal audit (IoD, 2002:79; IoD, 2009b:73, 75, 80). CIOs also have a shared responsibility with risk management, since they have a deep understanding of technology and how it interacts with business processes (Nash, 2011). The CIO’s IT planning, budgeting and performance activities should always be supported by risk management (Stoneburner, et al. 2002:6). Ideally, risk management planning for IT security threats and risks that obviously includes hacking should not be performed by the organisation’s security experts in isolation. The board, audit committee, senior management or internal audit should be involved in the process of risk management, and this also holds true in respect of IT risks and hacking. Even though these role-players may not have detailed technical knowledge of IT and hacking, they need to understand the nature of IT security threats and risk and how it may affect their business (Lipson & Fisher, 2000:35-36).

Research into audit committees at Top 40 JSE-listed companies has revealed that at the largest listed companies in South Africa, this is a real concern. This research revealed that from the perspective of CFOs, 64,7% believed that their audit committees were effective to a lesser extent in discharging their IT governance responsibilities (Marx, 2008:390), while the same percentage of audit committee chairpersons also believed that their audit committees
were less effective in this matter (Marx, 2008:407). Marx comments that even though audit committees at large listed companies in South Africa are effective in many respects, the extent to which they are able to address IT matters is questionable (Marx, 2008:408). It is therefore questionable whether audit committees will have sufficient insight into the threat of hacking.

Recent research commissioned by COSO into the current state of ERM has highlighted the immaturity of ERM among respondents. The research was conducted by the ERM Initiative at the North Carolina State University during the US summer of 2010. A total of 460 executives completed an online survey. Respondents were mostly from the finance, manufacturing, insurance and real estate industries. In answer to the question as to the level of maturity of the organisation’s ERM process, 14.5% indicated “very immature” and 27.9% indicated “somewhat immature”. As to whether a member of senior management has been given the responsibility of co-ordinating ERM in the organisation, 24.3% indicated “not at all”. In respect of the formation of a dedicated subcommittee for risk oversight, 38.5% indicated that they did not have a committee in place. The COSO ERM framework was regarded as the best-known ERM framework (54.6% of respondents), while other frameworks, such as ISO 31000:2009 (1.9% of respondents) received significantly lower responses (Beasley, et al. 2010:iii, 2, 6). This indicates low maturity levels of ERM in organisations, which may affect an organisation’s ability to identify risks. A further contributing factor to this may be that CIOs are not embracing ERM and are not assisting management by consolidating disparate risk data or by providing guidance as to the most appropriate technical solution towards ERM (Burnes, 2008).

5.4.6 Advantages of the risk management or ERM response

There are several benefits to be derived from risk management in that it enhances the organisation’s control environment. It also aids in avoiding detrimental scenarios which may result from hacker attacks, increasing the organisation’s operational or reputational risk. The risk management process also protects shareholder value, while investors and customers would display increased levels of trust with the presence of a risk management function. It supports corporate governance practices, while serving as early warning for detecting new and increased risk levels. A risk management function increases an organisation’s competitive advantage and will lead to a more structured risk management process, if there is recognition by the board of directors of the importance of risk management (Schönfeldt, 2000:14-15). The risk management process could assist in determining the impact and likelihood of the risk of hacking, which may assist in identifying an appropriate mitigating
strategy or response.

There are several specific benefits to be derived from managing IT risk and security with an ERM approach (McClean, et al. 2010:2-3):

- A risk assessment aids in the prioritisation of risk and mitigation approaches. Ethical hacking, for example, could identify several vulnerabilities. The risk assessment could aid with the prioritisation of the vulnerabilities. Consequently, it may potentially mitigate the hacker threat.
- Through risk quantification, investment decisions can be justified. By quantifying the potential loss due to a hacker attack, the necessary funding can be obtained to address the security weaknesses.
- IT risks can be associated with affected assets and business processes. In doing so, the board of directors will have an understanding of how their organisation is affected by hacker attacks.

When monitoring the risk of hacking as part of ERM, the likelihood and impact of hacking will be determined across the organisation, and a co-ordinated mitigating response could be formulated. A consolidated view provided by ERM would also be beneficial to the board of directors, who could better direct resources to the real problem areas. Given the integration of IT risk with the other business risk categories and its integration with hacking, such an integrated approach to risk management will be invaluable in identifying, managing and monitoring risk.

5.4.7 Disadvantages of the risk management or ERM response

Risk management processes could focus on identifying traditional business risks, which might exclude the risk of hacking or alternatively might focus less on IT risks in general. The risk management process might not focus on granular risks and might be ineffective in identifying the generic IT risks identified in this thesis (Table 4.25). Since risk management frameworks do not recommend which risks to focus on, the identification of relevant business risks (including IT risks) will depend on the knowledge and expertise of those responsible for identifying significant risks (Committee of European Banking Supervisors, 2010:5). Therefore, the possibility exists that the risk of hacking might not be identified or might not be recognised as a significant IT risk.

In a survey commissioned during 2010 by COSO into the board of director’s risk oversight responsibilities, completed by 200 board members, mostly based in the USA, with a quarter
of the respondents from the financial services industry, the lack of commitment to establishing an ERM function was confirmed. Of the participating board members, 40% indicated that they have "more pressing needs", 31% indicated a lack of understanding ERM and a similar percentage discarded the value to be derived from ERM (Protiviti & COSO, 2010:3, 13). In particular, it has been highlighted that 68% of public companies review risks of a high impact and low likelihood only periodically (Protiviti & COSO, 2010:11). The risk of hacking could fall into this category. ERM processes focus specifically on identifying significant organisational risks and establishing whether the corresponding internal controls have been implemented to mitigate those key organisational risks (IRMSA, 2007:32). The disadvantage of this is that risk practitioners might have a difference in opinion as to what is considered a significant organisational risk. The risk of hacking might be regarded as negligible (rightly so for organisations that do not rely on IT). However, if the risk of hacking is underestimated or simply not identified due to a lack of knowledge or expertise, the organisation might be exposed to hacker attacks.

5.4.8 Risks addressed by the risk management or ERM response

Risk management or ERM is a process aimed at identifying significant organisational risks. It does not focus on any particular business or IT risk. Due to the universal nature of the business risks identified in this thesis, there is a high likelihood that they will be included in an organisation’s inventory of risks. Whether or not all of the IT risk themes (Table 4.25) will be identified by the risk management or ERM processes will depend on the significance of the IT risks within the context of the particular organisation’s risk environment. Risk management or ERM can be a direct response to the risk of hacking, if the risk of hacking is in scope for the particular organisation. As for the coverage of the control objectives, since a possible response towards mitigation of particular risks may include the implementation of internal controls, it is possible that one or more of the control objectives may be covered.

5.4.9 Conclusion

The risk management or ERM process could be effective in identifying the risk of hacking, if hacking is considered significant in the context of the organisation’s business and if the required risk identification expertise is available within the organisation. To ensure identification, the IT risks need to be within the scope of the organisation’s risk environment. The risk management process could then be effective in assessing the impact and likelihood of hacking incidents. The close alignment with corporate governance will ensure that significant risks will be brought to the attention of the board of directors and may result in an
increase of resources or funding to mitigate the risk of hacking. Then again, the possibility exists that the risk of hacking is not recognised as part of an organisation’s risk management process, due to a lack of evidence or inability to contextualise the significance and probability of the risk. This may expose the organisation to hacker attacks.

Risk management does not focus on managing or detecting hacking events as they occur, since it has a forward-looking approach towards risks materialising in the future and is therefore preventative in nature. In addition, risk management or ERM may only be effective in identifying the risk of hacking, when it is augmented by additional supporting processes, such as ethical hacking (as is the case with the risk management framework, NIST SP 800-30) to increase the likelihood of recognising the significance of the risk of hacking.

**Thematological research questions**

Based on the literature review above, the following thematological research questions can be defined:

**Corporate governance**
- The extent to which risk management is used in the banking sector to manage IT risk.
- The extent to which the risk management process is used to create awareness among the board of directors regarding the significance of IT risk and hacking in particular in the banking sector.
- The extent to which the key role-players, ranging from the board to the CEO and the CIO, are involved in risk management processes in the banking sector.
- Whether the banking sector makes use of ERM, as opposed to a standalone risk management process.
- Whether the board of directors has the required knowledge to assess the risk of hacking as part of the ERM process in the banking sector.
- Whether the banking sector has the required expertise to identify the risk of hacking as part of its risk management process.

**IT risk**
- The extent to which hacking is considered an IT risk, during the risk management process in the banking sector.

**Hacking response**
- Whether risk management or ERM is used towards the identification of the appropriate response for the risk of hacking in the banking sector.
- Whether risk management or ERM has been successful in mitigating the risk of hacking in the banking sector.
- The extent to which specific risk management methodologies, such as NIST SP 800-30, are used to address the risk of hacking in the banking sector.
- The extent to which the systematic and continuous process for risk management addresses hacking in the banking sector.
- The extent to which there is recognition in the banking sector that a formal risk management approach may be employed to address IT risk and specifically hacking, and the extent to which this response is utilised.
5.5 HACKING AND THE INTERNAL CONTROL RESPONSE

5.5.1 The essence of the internal control response

Internal control is the “basis for effective operational and accounting business processes” (Moeller, 2009:23). Internal control is also defined as (SAICA, 2007:ISA 315.4; Cosserat & Rodda, 2009:711; Marx, et al. 2009:12.3):

The process designed and effected by those charged with governance, management and other personnel to provide reasonable assurance about the achievement of the entity’s objectives with regard to reliability of financial reporting, effectiveness and efficiency of operations and compliance with applicable laws and regulations.

The board of directors or senior management might set strategic objectives for the organisation and internal control could possibly assist the organisation in achieving those objectives. Despite this, internal control might not always be a key priority for management when managing the business (Moeller, 2009:25). Nonetheless, management remain responsible for implementing internal control (Marx, et al. 2009:12.6; Moeller, 2009:24) and also implementing monitoring to ensure the effectiveness of internal control (IIARF, 2009:6.13).

A system of internal control is a key requirement of a healthy system of corporate governance (Cortesi, Tettamanzi & Corno, 2009:81). It is not a framework as such, but rather a process or mechanism to respond to business and IT risk. Internal controls can assist with the mitigation of a diverse range of business risks across an organisation (Pickett, 2010:273). Although internal control does not provide absolute protection, it could assist an organisation in achieving its corporate governance objectives, through avoiding material errors and losses, fraud, and breaking laws or regulations (Deloitte & Touche LLP, 2003:3, 7, 10, 27). Important aspects to consider since the lack of internal control was one of the key root causes behind well-known corporate governance failures (Piti, 2004:16).

It has already been highlighted that responses to risk include avoiding, mitigating, transferring, accepting, exploiting, terminating and integrating the risks (IoD, 2009b:78). Internal control provides directive, detective, preventative and corrective responses (as discussed in section 4.3.5.11). It is clear that it does not provide the same range of responses as would be required to respond to risks.

To illustrate the focus on internal control in the financial services industry as a response to
the absence of control or business risks (including IT risks), a number of well-known international frameworks, which highlight the importance of internal control as a response to business risk and other associated risks, will be considered. The frameworks presented here do not recommend any specific internal controls. Instead they support the use of internal control:

- COSO places emphasis on internal control as a process, to ensure the effectiveness and efficiency of operations, reliability of financial reporting, and compliance with legislation and regulations (Eslami, *et al.* 2007:75). From a COSO perspective, internal controls include IT and information security controls (Whitman & Mattord, 2008:235).

- The criteria for control (hereafter CoCo) is an international standard developed by the Canadian Institute of Chartered Accountants (hereafter CICA). It consists of a model that focuses on the purpose, commitment, capability, action, and monitoring and learning towards establishing internal control. The model also distinguishes between scientific (hard) and humanistic (soft) controls (Pickett, 2010:264-267).

- Basel II sets out a comprehensive measure and minimum standard for capital adequacy, including a supporting risk management process. It requires an independent review of the internal control structure that supports the capital assessment process. From an IT risk perspective, it requires specific attention to the accuracy and completeness of data inputs into the bank’s risk assessment process (Basel, 2004:1, 162). Basel III is a revision of bank capital adequacy and liquidity requirements and sets new regulatory standards. It is aimed at increasing financial stability and increased risk coverage. It encourages a phased migration approach towards Pillar 1 treatment by the end of 2017 (Basel, 2011).

- SOX is legislation applicable to companies listed on the US stock exchanges and also sets corporate governance standards for management and public accounting firms. Its aim is to strengthen corporate accountability, improve audit independence and integrity, empower audit committees, and protect employers, pension holders and investors from fraud and accounting errors. This is supported by a robust system of internal control (Biegelman & Bartow, 2006:63, 64; Larsen, *et al.* 2006:3). Although SOX is not mandatory in South Africa per se, Securities & Exchange Commission registered organisations, either “subsidiaries of US domestic registrants or foreign private investors”, have to comply with SOX (PwC, 2011).

It is submitted that the use of internal control as defined in COSO is commonplace in the financial services industry and the banking sector in particular. Basel II is also used comprehensively in the South African banking sector (Bostander, 2007:13) and increasingly
banks will also adopt Basel III, as many South African banks already surpass the Basel III capital adequacy requirements (Faure, 2011). The highly complex nature of the banking sector requires a mature internal control environment, which will also aid in managing hacking risks and events. In order to determine the effectiveness of internal control, control objectives identified in this thesis can be used as measurement to assess the effectiveness. The control objectives are applicable to business and IT risks.

5.5.2 Application of the internal control response

Internal control could be the end product of a risk assessment exercise, where a particular risk is mitigated by applying internal control. By improving the control environment, the corresponding risk will be reduced or mitigated (Charette, 2005:3; IoD, 2009b:78). The IT risk themes can therefore be addressed by implementing resultant internal control, while the control objectives can be used to measure the effectiveness of the internal control. Similarly, specific internal control can be defined and implemented to address the threat of hacking. As will be discussed in section 6.9.4.1, ethical hacking is effective in identifying appropriate internal control to mitigate the threat of hacking.

5.5.3 Dimensions of the internal control response

Internal control is generally regarded as the “first line of defence”, followed by management oversight and thirdly independent assurance (ZAO KPMG, 2009:1-3). Internal control is a direct response to business risks, including IT risk and hacking. It is the foundation of an organisation’s control environment. The frameworks included in this section (COSO, Basel II and SOX) do not define detailed control objectives and cannot be used as a direct response to hacking. They all however support the use of internal control. Internal control focuses on both the event and risk of hacking. Similarly, internal control could be preventative or detective in nature.

5.5.4 Role-players in the internal control response

There are numerous role-players who ensure internal control. The board of directors carries the overall responsibility for internal control (IoD, 2009b:31; Braiotta, Gazzaway, Colson & Ramamoorti, 2010:239). It is however management who will implement internal control and report back to the board of directors on the effectiveness thereof (IoD, 2002:86; Charette, 2005:2). Another key role-player is internal audit, which is responsible for assessing internal control, with oversight by the audit committee (IoD, 2002:90; IoD, 2009b:63, 93). The
effectiveness of the internal audit function also contributes towards the overall effectiveness of internal control (Cortesi, et al. 2009:82). Indirectly, the audit committee also plays a role, in that it provides oversight over the accounting and financial reporting processes, as well as the effectiveness of internal and external audit (Braiotta, et al. 2010:239). External audit may engage with the risk committee, internal audit and the Chief Risk Officer (hereafter CRO) to determine whether reliance can be placed on the internal controls (with a focus on financial controls) (IoD, 2009b:80). Although not specifically mentioned as being responsible for internal control, the CIO should engage with the board of directors on matters of IT governance. It follows that an “IT internal control framework” is established within the context of IT governance (IoD, 2009b:82, 84). The CIO will therefore also be responsible for internal control. Management is however responsible for implementing internal control, including internal controls that will address the threat of hacking. SOX requires the CEO and the CFO to assume direct and personal accountability for the accuracy and completeness of an organisation’s financial reporting and record-keeping systems. The CEO or CFO will place reliance on the CIO, who is responsible for the security, accuracy and reliability of IT systems that support the financial reporting (Whitman & Mattord, 2008:449). In effect, all levels of management are responsible for defining and implementing internal control, although senior levels of management will play more of an oversight role.

5.5.5 Advantages of the internal control response

Internal control has several advantages, such as increasing the effectiveness of operations, achieving cost savings through control efficiencies, pinpointing and deterring irregularities, and protecting assets and resources (Port Pirie Regional Council, 2009:4). When automated, and also applicable as a response to the threat of hacking, internal controls can “reduce the risk that controls will be circumvented” and enable segregation of duties by implementing security controls at application, database and operating system level (SAICA, 2007:ISA 315:A55). Automation also removes the human element, which may decrease the risk further. Internal control therefore provides an essential first layer response against the threat of hacking.

5.5.6 Disadvantages of the internal control response

Although internal control defines a direct and immediate response to a particular risk, the reality is that internal control can only provide “reasonable assurance” and not absolute assurance against the threat of hacking (Cangemi & Singleton, 2003:69). There are inherent limitations associated with internal control, such as the failure in human judgement, a
breakdown of internal control due to human error and lack of segregation of duties. Even with the most effective controls in place, internal controls can still be circumvented (SAICA, 2007:ISA315.A46, A47; Marx, et al. 2009:12.8; IIARF, 2009:6.18). It is particularly here where the creative nature of hackers plays a role in that they will find ways to circumvent the internal controls. They will follow the path of least resistance, or bypass the controls and find weaknesses in the organisation’s defences where the organisation least expects it. Internal control then potentially becomes completely ineffective. Although automation has clear benefits, it may also increase risk, in that it may lead to unauthorised access and consequent destruction of data, or unauthorised changes to data, programs and systems (SAICA, 2007:ISA315.A56). As noted in this thesis, hackers can be the source of those risks materialising.

5.5.7 Risks addressed by the internal control response

Internal control or the frameworks encouraging the use of internal control do not provide guidance as to which risks to focus on. Rather, in establishing a “sound system of internal control”, organisations need to assess the “nature and extent of the risks” faced by the organisation (IoD, 2010:2). Similar to control objectives identified in this thesis, internal control is the opposite of risk, or alternatively a direct response to a particular risk. Table 5.2 reflects internal control for each IT risk theme, which can be seen as a corollary for each IT risk theme. The table reflects only one permutation of internal control and is merely an example to illustrate the point, since many possible internal controls could be defined for each IT risk theme. The control objectives can further augment the objective to be achieved by each internal control. This is evident given that control objective terms, such as “authorised” and “securely”, are contained within some of the internal control statements.

Table 5.2 Internal control as a response to IT risk themes (own interpretation)

<table>
<thead>
<tr>
<th>General controls:</th>
<th>Internal control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorised physical access / lack of physical access control and security.</td>
<td>Authorised physical access / physical access control and security.</td>
</tr>
<tr>
<td>Lack of compliance with IT policies and procedures, legal and regulatory requirements.</td>
<td>Compliance with IT policies and procedures, legal and regulatory requirements.</td>
</tr>
<tr>
<td>Business and IT disruption.</td>
<td>Disaster recovery / business continuity.</td>
</tr>
<tr>
<td>Inadequate IT operations and support.</td>
<td>Effective IT operations and support.</td>
</tr>
<tr>
<td>Theft or damage to IT equipment.</td>
<td>Protection of IT equipment.</td>
</tr>
<tr>
<td>Inadequate change / project management practices.</td>
<td>Effective change / project management practices.</td>
</tr>
<tr>
<td>Misuse of IT / irregularities and fraud.</td>
<td>Monitoring the use of IT resources.</td>
</tr>
<tr>
<td>Cybercrime.</td>
<td></td>
</tr>
<tr>
<td>Unauthorised logical access.</td>
<td>Authorised logical access.</td>
</tr>
<tr>
<td>Inadequate IT performance.</td>
<td>Monitoring IT performance levels.</td>
</tr>
<tr>
<td>Complexity of IT.</td>
<td></td>
</tr>
</tbody>
</table>
Inefficient use of IT resources.  
IT human resource deficiencies.  
Application controls:
- Application control weaknesses.
- Data control weaknesses.
- Interface / network control weaknesses.
- Operating system weaknesses.
- Lack of an audit trail.
- Lack of segregation of duties.

<table>
<thead>
<tr>
<th>Inefficient use of IT resources.</th>
<th>IT resource planning and allocation.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT human resource deficiencies.</td>
<td>IT recruitment practices.</td>
</tr>
<tr>
<td>Application controls:</td>
<td></td>
</tr>
<tr>
<td>Application control weaknesses.</td>
<td>Application controls.</td>
</tr>
<tr>
<td>Data control weaknesses.</td>
<td>Data controls.</td>
</tr>
<tr>
<td>Interface / network control weaknesses.</td>
<td>Interface controls.</td>
</tr>
<tr>
<td>Operating system weaknesses.</td>
<td>Securely configured operating systems.</td>
</tr>
<tr>
<td>Lack of an audit trail.</td>
<td>Audit trails.</td>
</tr>
<tr>
<td>Lack of segregation of duties.</td>
<td>Segregation of duties.</td>
</tr>
</tbody>
</table>

5.5.8 Conclusion

Internal control is required by corporate governance as a response to business risk, which includes IT risks. The frameworks, standards or legislation associated with the internal control response do not provide detailed guidance on the mitigation of business, IT or hacking risks. Instead they support the principle of internal control. Internal control could be a direct response to business risks and IT risks (including hacking); however, internal control can be circumvented, which is often the case with hackers or insiders. The internal control implemented to prevent and detect hacker threats should be assessed to determine its effectiveness.

Thematological research questions

Based on the literature review above, the following thematological research questions can be defined:

**Hacking response**
- The extent to which internal control is used as the primary response against the threat of hacking in the banking sector.
- Whether there is realisation in the banking sector that internal control is not an absolute response against the threat of hacking.
- Whether the banking sector tests internal control in order to assess its effectiveness.

5.6 HACKING AND THE IT GOVERNANCE RESPONSE

5.6.1 The essence of the IT governance response

It is argued that IT risks (including the risk of hacking) do not originate from technical or employee issues, but rather from the lack of sufficient management oversight and poor IT governance (Westerman & Hunter, 2007:7). This increases the likelihood for IT risk emerging and negatively affecting the business potential derived from IT (Westerman & Hunter, 2007:7). A detailed discussion of the origin and need for IT governance has been
presented in section 2.6 and will be augmented here by the presentation of a definition to recap the purpose of IT governance (Rudman, 2008:12):

A framework to direct, manage and control the use of IT by encouraging an ingrained pattern of worthwhile behaviour for administrators and users alike with regard to acceptable practices, which sustain and extend an organisation’s strategies and objectives, while also mitigating IT-related risks.

IT governance is essentially about executive management’s ability to control IT’s strategic impact, while delivering value for business (Simonsson & Johnson, 2006:1). IT governance facilitates the balancing act between the risks and benefits derived from IT. IT governance is an essential sub-component of corporate governance (Bloem, van Doorn & Mittal, 2006:3, 11; Rudman, 2008:12). IT strategy, defined through IT governance processes, has to be aligned with business strategy and this strategy has to be imbedded into the organisation (Wailgum, 2010:34), while identifying the IT decision-makers and assigning accountability (Weill & Ross, 2005:26). King III requires the CEO to appoint a CIO, who is responsible for ensuring that the interrelationship between IT and business is achieved. Furthermore, the CIO needs to focus on the business aspects, to ensure that long-term business objectives are underpinned by effective IT solutions. The CIO therefore needs to think strategically about integrating IT into business and developing IT systems which meets the long-term objectives of the organisation (IoD, 2009b:84).

Effective IT governance will address business risks associated with IT and will provide assurance that an organisation’s strategic information is secure and reliable, and that information integrity is achieved. It will also ensure that IT investments, including IT systems and networks, are protected. It will further ensure that the organisation’s information assets will be appropriately managed, to guarantee the success and continued existence of the organisation (Lainhart, 2001:19).

In essence, an organisation’s IT assets should be protected against hacking incidents. The appropriate mechanisms should be implemented to respond to the risk of hacking. IT governance frameworks will help an organisation to achieve this objective. Although many frameworks are at times categorised as IT governance tools or frameworks (Larsen, et al. 2006:2-4; Bloem, et al. 2006:3; Rudman, 2008:13; Stoller, 2008:47), there are authoritative sources, such as King III and ISACA’s CGEIT qualification, which are more selective in their identification of IT governance specific frameworks, and these are outlined next (IoD, 2009b:16; Pankey, 2010:4, 7):

- The International Organization for Standardization / International Electrotechnical
Commission (hereafter ISO/IEC) 38500:2008 advisory standard provides a high-level framework to improve the governance of IT in an organisation (Calder, 2008b:11). The standard provides guiding principles to the board of directors on the effective and efficient use of IT (Calder, 2008b:15) and requires the board of directors to carry out three main actions: evaluate, direct and monitor (Calder & Moir, 2009:80).

- The Val IT framework assists organisations in achieving value from their IT investment (ITGI, 2008b:7, 9). Val IT ensures that IT investments are managed as a portfolio of investments (ITGI, 2008b:11). The Val IT framework consists of three core domains: value governance, portfolio management and investment management (ITGI, 2008b:15).

- CobiT 4.1 provides a framework for IT governance and information security management, through a consistent control model. It defines detailed IT control objectives, with various links back to IT goals and business objectives (Whitman & Mattord, 2008:232-235; ISACA, 2010b). CobiT 4.1 focuses on five key areas of IT governance: strategic alignment with business, value delivery towards maximising business benefits, effective utilisation of IT resources, managing IT risks appropriately, and setting and monitoring measurable objectives (Moeller, 2008:121; Greenfield, 2007; ITGI, 2007a:6). CobiT 5, released April 2012, is a new IT governance guide, considerably revised from CobiT 4.1. It contains 37 processes, broadly divided into IT management and IT governance processes (ISACA, 2012a:15).

Of the three frameworks listed above, only CobiT is a multipurpose framework, in that it defines both high-level principles and decision-making structures for IT governance, as well as providing detailed control objectives, whereas the other two frameworks only provide high-level IT governance principles.

### 5.6.2 Application of the IT governance response

IT governance ensures that an organisation’s IT function assists with the achievement of organisational objectives (ITGI, 2007a:5). IT governance also enables the integration of responses to the hacking threat into the organisation’s objectives. This ensures that the response to the hacking threat becomes a business imperative, rather than just a response to the hacking threat. It will also create greater awareness in the business user community and perhaps also increased vigilance. An IT governance response will also ensure integration with corporate governance and lift the response to hacking from an operational level to a corporate governance level.
ISO/IEC 38500 only provides a high-level framework for IT governance, without providing detailed control objectives. It can therefore not be applied as a direct response to hacking. Similarly, Val IT focuses on providing high-level guidance for increasing the value derived from IT investments and can also not be applied as a direct response to hacking. CobiT supports the Val IT framework to ensure the effective governance of IT. Each role-player in an organisation is given a role description and responsibility to ensure investment objectives are achieved (ITGI, 2008b:28, 29).

CobiT is a highly applicable response to the hacking threat. CobiT provides a balance between clearly linking business requirements, IT processes and IT resources, while providing an overall framework and high-level objectives, to provide a comprehensive IT governance framework (Moeller, 2008:127). At the same time, it defines key controls at a low enough level, to allow the controls to be operationalised in any organisation (Wessels, 2006:42). The wide use of CobiT in general in financial services organisations and highly IT-dependent industries (Simonsson & Johnson, 2006:1) highlights the significance, applicability and ease of use of CobiT. With a further strong focus on IT risk management and broad coverage of IT risks in an organisation, the addition of CobiT becomes highly applicable as a response to hacking. CobiT deals with the risk of hacking at a control level, while reporting on it at an IT control objectives level and also closely aligning with business objectives. This close alignment of the CobiT framework with business objectives could assist business executives to comprehend the true impact of IT risks, such as hacking.

5.6.3 Dimensions of the IT governance response

When applying IT governance, through a framework such as CobiT, which provides detailed control objectives, IT governance provides a direct response to IT risks and hacking. CobiT is both preventative and detective in nature (Flowerday & Von Solms, 2005:609), since it defines IT operational processes for IT security which are preventative and also encourage establishing monitoring processes which are detective in nature. Not only will CobiT be effective in addressing the IT risks themes, it will also address the risk of hacking at a lower level. CobiT has its own detailed control objectives, although many of them only provide a process response, will be explained in section 5.6.7.

5.6.4 Role-players in the IT governance response

There are various role-players in IT governance, due to the pervasive nature of IT in business. Role-players include the board of directors, the CIO, senior or executive
management and IT management (Peterson, 2004:9; Weill & Ross, 2005:26; Goeken & Alter, 2007:1, 2; IoD, 2009b:84). CobiT emphasises that the board of directors and executive management are ultimately responsible for IT governance (ITGI, 2007a:5). Key role-players involved in the Val IT framework are the board of directors, executive management and “other enterprise leaders” (ITGI, 2008b:8, 9). ISO/IEC 38500 encourages the participation of the board of directors, directors in general and management (ITGI, 2009:8-10). Most notable is that these are mostly senior members of staff in an organisation, which indicates that operational staff might not be directly involved in the strategic IT governance decisions. This may impact the likelihood of identifying hacking at a technical level and reporting it at a governance level.

5.6.5 Advantages of the IT governance response

IT governance is considered to deliver a greater return on IT investment, while enabling a competitive advantage among industry rivals (Calder, 2007:35). It improves risk management practices and delivers value for IT investments (Williams, 2006:26). IT governance could lead to consolidated decision-making, thus preventing managers from making decisions in isolation (Weill & Ross, 2005:26). It is submitted that IT governance may ensure an integrated pervasive response to the threat of hacking, rather than a silo-based approach and disparate decision-making.

As an IT governance framework, CobiT is increasingly seen as a best practice benchmark for managing risk and defining controls to manage IT processes and IT investments. It is favoured by business executives, due to its strong focus on business objectives. This also makes it accessible to non-IT literate business executives (Lainhart, 2001:19-20). CobiT can assist management in establishing an IT governance framework for an organisation (Senft & Gallegos, 2009:220).

The best practice framework, Val IT, is beneficial to organisations that seek business value from their IT investments. It is also complementary to CobiT (ITGI, 2008b:6) and provides practical process details. ISO/IEC 38500 is beneficial as a high-level guidance framework for IT governance and emphasises the importance of IT governance to key stakeholders (ITGI, 2009:7).
5.6.6 Disadvantages of the IT governance response

There are various definitions and interpretations of IT governance (Simonsson & Johnson, 2006:1), which may lead to differences in understanding the concept and various opinions among stakeholders on how it should be implemented. The implementation of IT governance is at times overcomplicated, leading to implementation failures (Sylvester, 2011). In itself, IT governance is not a direct response to the threat of hacking. IT governance may therefore ensure strategic direction, but lack mobilisation at an operational level. The response will have to be enabled through a framework, such as CobiT, to provide a more granular-level response.

As discussed in section 5.6.1, there are also numerous frameworks, tools and models available, classified under the IT governance umbrella. This could complicate the implementation of IT governance, since a decision will have to be made as to the best supporting framework (Eslami, et al. 2007:73; ISACA, 2010a:27). The various frameworks are also not necessarily complementary to each other and may lead to duplication or overlap between various frameworks (Pankey, 2010:5). There may also be a certain skills level associated with a particular framework, which, depending on the size and complexity of the organisation, might be too expensive or too specialised to deploy.

CobiT defines organisational processes, without providing implementation guidelines. CobiT may have to be augmented by other responses, such as IT security baselines or ethical hacking, for a more granular response.

A possible disadvantage of Val IT is that it has been defined as an extension of CobiT, rather than a standalone IT governance framework. Val IT focuses predominantly on the business value and investment component of IT (ITGI, 2008b:6) and does not provide comprehensive coverage of all IT governance related aspects. A possible disadvantage of ISO/IEC 38500 is that it is a high-level framework, which provides high-level guiding principles (ITGI, 2009:7), without providing guidance on how to implement the high-level principles. Organisations may therefore find it challenging to implement ISO/IEC 38500.

5.6.7 Risks addressed by the IT governance response

In itself, IT governance does not focus on any particular risk, but rather encourages the use of risk management practices, or needs to be augmented by specific frameworks towards identification of IT risks.
ISO/IEC 38500 provides a high-level framework for IT governance, towards alignment of IT and business goals (Gopinath, 2009:4; Badenhorst, 2009:9). It therefore does not address hacking directly; however, indirectly IT governance processes will be imbedded and improved towards managing IT risks and events throughout the organisation, which may include hacking risks or events.

Although Val IT is fundamental from an IT governance perspective in ensuring that value is derived from IT investments, it cannot be used as a direct response to the IT risk themes or the risk of hacking. Indirectly it could be used to channel funds to solutions and processes which will aid in the mitigation of the hacking threat. It is therefore preventative in nature, since current investments will mitigate future hacking events (the risk of hacking).

However, CobiT provides detailed control objectives, which can be used as a direct response to the IT risk themes (refer Table 5.3). It should be considered that the response is mostly in the form of processes that could address a particular risk. A more detailed mitigating response or internal control will have to be defined within those processes. CobiT does not distinguish hacking risks specifically, but by implication they will be addressed due to their close association with the IT risk themes, as shown in chapter 4. CobiT’s information criteria, which are aimed at assisting an organisation in achieving its business objectives, include the control objectives confidentiality, integrity and availability (ITGI, 2007a:10-11).

Table 5.3  CobiT 5 as a response to the IT risk themes (own comparison)

<table>
<thead>
<tr>
<th>General controls:</th>
<th>CobiT 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorised physical access / lack of physical access control and security.</td>
<td>DSS05.05 Manage physical access to IT assets</td>
</tr>
<tr>
<td>Lack of compliance with IT policies and procedures, legal and regulatory requirements.</td>
<td>EDM01.01 Evaluate the governance system APO01.08 Maintain compliance with policies and procedures MEA03 Monitor, Evaluate and Assess Compliance with External Requirements</td>
</tr>
<tr>
<td>Business and IT disruption.</td>
<td>DSS04.03 Develop and implement a business continuity response DSS04.05 Review, maintain and improve the continuity plan</td>
</tr>
<tr>
<td>Inadequate IT operations and support.</td>
<td>APO09 Manage Service Agreements</td>
</tr>
<tr>
<td>Theft or damage to IT equipment.</td>
<td>DSS01.04 Manage the environment DSS01.05 Manage facilities DSS05.05 Manage physical access to IT assets</td>
</tr>
<tr>
<td>Inadequate change / project management practices.</td>
<td>BAI01.01 Maintain a standard approach for programme and project management</td>
</tr>
<tr>
<td>Misuse of IT / irregularities and fraud.</td>
<td>DSS05 Manage Security Services</td>
</tr>
<tr>
<td>Cybercrime.</td>
<td>DSS05 Manage Security Services</td>
</tr>
<tr>
<td>Unauthorised logical access.</td>
<td>DSS05.04 Manage user identity and logical access</td>
</tr>
<tr>
<td>Inadequate IT performance.</td>
<td>MEA01 Monitor, Evaluate and Assess Performance and Conformance</td>
</tr>
<tr>
<td>Complexity of IT.</td>
<td></td>
</tr>
</tbody>
</table>
Inefficient use of IT resources. | APO06 Manage Budget and Costs
---|---
IT human resource deficiencies. | APO07.01 Maintain adequate and appropriate staffing  
APO07.05 Plan and track the usage of IT and business human resources  
EDM04.02 Direct resource management

Application controls:

| Application control weaknesses. | BAI03.05 Build solutions
| Data control weaknesses. | DSS06.02 Control the processing of information
| Interface / network control weaknesses. | DSS05 Manage Security Services
| Operating system weaknesses. | DSS05 Manage Security Services
| Lack of an audit trail. | DSS05 Manage Security Services
| Lack of segregation of duties. | DSS06.03 Manage roles, responsibilities, access privileges and levels of authority

5.6.8 Conclusion

Within the highly automated business environments of today, IT governance has become an imperative to drive IT delivery towards meeting business objectives. When IT governance is used as a response to the IT risk themes and hacking, the focus shifts from responding to those risks at an operational level to responding to them at a governance level. Nonetheless, the impact of IT governance also needs to feed through to the operational level, which is enabled by a framework, such as CobiT, which provides not only a high-level IT governance framework but also detailed control objectives which can be operationalised as a response to the IT risk themes, including hacking. IT governance is therefore a highly applicable response to the threat of hacking, albeit mostly at a process level.

Thematological research questions

Based on the literature review above, the following thematological research questions can be defined:

**IT Governance**
- The extent to which there is an understanding of IT governance frameworks at board level in the banking sector.
- Whether a particular individual has been assigned the responsibility for IT in the banking sector.
- Whether the CIO or individual responsible for IT clearly understands the strategic objectives of the banking sector.
- The extent to which there is recognition in the banking sector that there is a need for IT governance and IT governance frameworks.
- The extent to which boards of directors are involved in selecting and monitoring the application of IT governance frameworks in the banking sector.
- Whether there is a clear understanding in the banking sector of the various IT governance frameworks and what each can and cannot be used for from an IT governance perspective.

**Hacking Response**
- The extent to which IT governance frameworks are applied as a response to hacking in the banking sector.
- The extent to which there is an understanding in the banking sector of which IT governance framework is
the most appropriate in addressing the threats posed by hacking.

- The extent to which CobiT, Val IT and ISO/IEC 38500 in particular are used as direct responses to the risk of hacking in the banking sector.
- The extent to which multiple frameworks are used in the banking sector to provide a comprehensive response to the risk of hacking.

5.7 HACKING AND THE SERVICE MANAGEMENT RESPONSE

5.7.1 The essence of the service management response

Service management, from an IT perspective, deals with providing efficient and effective service support and service delivery as a distinguishing factor from other potentially competing IT service providers (Hochstein, Zarnekow & Brenner, 2005:1, 2). It is also defined as “a set of specialized organizational capabilities for providing value to customers in the form of services” (IT Service Management Forum, hereafter itSMF, 2007:6). IT service management is a subset of IT governance and two frameworks commonly associated with IT service management is ITIL and ISO 20000 (Graves, 2010:1):

- ITIL provides international best practice recommendations on IT service management, divided into five core books, which cover service strategy, service design, service transition, service operation and continual service improvement (ITGI, 2008a:20; Klosterboer, 2009: 3, 4).
- ISO/IEC 20000:2005 is a service management standard providing guidance for a service management system (Clifford, 2010:8). ISO/IEC 20000 has been derived from the British Standard 15000, which in turn has been derived from ITIL (Galup, Dattero, Quan & Conger, 2009:125). Therefore, ISO/IEC 20000 has in effect been derived from ITIL (Wallace & Webber, 2009:17). ISO/IEC 20000 is regarded as the definitive standard for IT service management (Graves, 2010:2).

Both frameworks are essentially best practice service management frameworks. ITIL is perhaps a better-known framework than ISO 20000.

5.7.2 Application of the service management response

It is submitted that service management cannot be used as a direct response to the threat of hacking. Indirectly, ITIL and ISO/IEC 20000 could be used to manage an actual hacker incident. As part of the IT service management process, incident management is used to
restore service to its original state. During the incident management process, the hacker incident will be recorded and appropriate action will be taken to resolve all service disruptions (Wallace & Webber, 2009:18). Change management is another process defined by the service management discipline, which could be used to prevent unauthorised changes to the production environment (itSMF, 2007:25). This could prevent in particular insiders from introducing malicious code in the production environment.

5.7.3 Dimensions of the service management response

ITIL and ISO/IEC 20000 are regarded as detective in nature, since the incident management process engages only after the incident has occurred. It also focuses on the event, as opposed to the risk. The risk element could be addressed when the problem management process of ITIL or ISO/IEC 20000 is used to address the root cause of a system vulnerability being exploited by a hacker, thereby preventing future hacker attacks (Wallace & Webber, 2009:19). Control objectives are considered, for example, to ensure that all hacker incidents are recorded (completeness). By resolving the root cause, the control objectives availability and security are achieved. The maturity of the service management process might ensure smooth and timeous recovery. The lack of a service management process and the inability to recover quickly after a hacking incident might expose the organisation to further hacker attacks and reputational damage.

5.7.4 Role-players in the service management response

Key role-players defined in ITIL are the business relationship manager, product manager, Chief Security Officer (hereafter CSO), service design manager, IT architect, service catalogue manager, service level manager, availability manager, IT service continuity manager, capacity manager, security manager and supplier manager (itSMF, 2007:17, 23). These role-players are mostly found in the procurement or IT departments. Most of these role-players will not be involved in the response to hacking, except the availability manager, IT service continuity manager and security manager.

5.7.5 Advantages of the service management response

Deployment of IT service management through a framework such as ITIL increases end-user satisfaction with IT services, improves IT service availability, which equates to increased profits and financial savings, and leads to improvements in decision-making, while reducing risk (itSMF, 2007:8). From a hacking incident perspective, service management will
increase the speed of remediating a hacking incident.

5.7.6 Disadvantages of the service management response

In itself, the service management response is not a direct response to the risk of hacking. It does not define detailed control objectives which can be used to address the hacking threat at an operational level. It only provides a limited indirect response to hacking.

5.7.7 Risks addressed by the service management response

Since ITIL and ISO/IEC 20000 focus predominantly on IT service management, they do not cover the entire IT management discipline and have limited application in addressing business risks, IT risks or hacking across an organisation, but they remain important in IT service management. They may apply indirectly to hacking, when for example mature change management processes identify changes to production systems due to insider or hacker breaches. IT service management addresses the IT risk themes inadequate IT operations and support, inadequate change management practices, inadequate IT performance and inefficient use of IT resources. The most relevant control objective is availability, which further highlights the limited nature of the service management response.

5.7.8 Conclusion

Service management, a sub-component of IT governance, is primarily focused on managing IT incidents. It is not a direct response to the threat of hacking, but could be used to manage the consequences of a hacker incident. Service management only addresses four of the 16 IT risk themes. It therefore provides only a very limited and incomplete response to IT risk and the threat of hacking.

<table>
<thead>
<tr>
<th>Thematological research questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Based on the literature review above, the following thematological research questions can be defined:</td>
</tr>
<tr>
<td><strong>IT Governance</strong></td>
</tr>
<tr>
<td>• The extent to which the service management response is used to recover from hacking incidents in the banking sector.</td>
</tr>
</tbody>
</table>
5.8 HACKING AND THE QUALITY MANAGEMENT AND SOFTWARE DEVELOPMENT RESPONSES

5.8.1 The essence of the quality management and software development responses

There are several frameworks and models which focus on quality management, project management and software development, which have been identified as prominent during the literature review conducted for this chapter. Since all of them only provide an indirect response to hacking, they will only be covered briefly in this thesis:


- **CMMI** – The Capability Maturity Model Integration (hereafter CMMI) framework focuses on improving processes within an organisation. The framework defines five levels of maturity. The intention is that as members of a team mature in terms of their software development skills, they would move up to a higher maturity level. At each level, they need to master process areas which are divided into four categories: process management, project management, engineering and support (Anderson, 2001:522; ITGI, 2007b:18).

- **Six Sigma** - Six Sigma may be defined as: “… a business strategy that seeks to identify and eliminate causes of errors or defects or failures in business processes by focusing on outputs that are critical to customers. It is also a measure of quality that strives for near-elimination of defects using the application of statistical methods. A defect is defined as anything which could lead to customer dissatisfaction. The fundamental objective of the Six Sigma methodology is the implementation of a measurement-based strategy that focuses on process improvement and variation reduction” (Antony, 2008).

- **Balanced Scorecard** - A balanced scorecard is based on four principles: financial evaluation; customer satisfaction; internal processes and innovative ideas. Missions, objectives and measures are defined for each of the four principles for a particular organisational unit. These are each translated into a specific metric or measurement. Measurements are taken periodically and assessed against the original mission and objectives (Van Grembergen, De Haes & Amelincx, 2003:59; Cram, 2007:33).

- **TOGAF** - The Open Group Architecture Framework (hereafter TOGAF) is a standard
used to produce, approve and maintain architectures. It makes use of an iterative process model and a “re-usable set of existing architectural assets” (Josey, 2009:5). The framework can be used to define and develop business, data, application and technology architectures (Josey, 2009:6; Wallace & Webber, 2009:8).

- **SDLC** - The most basic SDLC originated in the 1970s when a need arose to develop software in a more structured approach. Over the years many interpretations have evolved as to what a SDLC should consist of. One interpretation is that it may consist of the following stages that are also often referred to as the “waterfall model”: feasibility study, system investigation, systems analysis, systems design, implementation, and review and maintenance (Avison & Fitzgerald, 1995:20).

- **PRINCE2** - PRojects IN Controlled Environment 2, better known as PRINCE2, covers a number of project management themes, which includes compiling a business case, project organisation, planning and controlling, project stage definition, management of project risks, instilling quality in the project environment and change control (Avison & Fitzgerald, 1995:206; Hughes & Cotterell, 1999:269-270; Bentley, 2006a:2-3; Crown, 2009:17).

- **PMBOK** – The Project Management Body of Knowledge (hereafter PMBOK) is recognised as a de facto standard in project management. It has several knowledge areas, which could be indiscriminately applied to any phase of an SDLC methodology. The knowledge areas include project integration, scope, time, cost, quality, human resource, communication, risk and procurement management (Hughes & Cotterell, 1999:317; Merna & Al-Thani, 2005:203; Project Management Institute, Inc. hereafter PMI, 2008:67).

Each of these frameworks has a unique focus, although the underlying themes are software development, project management and quality management practices.

### 5.8.2 Application of the quality management and software development responses

All of the frameworks listed above can only be used indirectly to address the risk of hacking: for example, ISO 9000 can assist with the mitigation of IT risk, since it improves IT governance processes (Barnier & Westerman, 2009:7). CMMI aids in improving software development practices overall, which could lead to more secure business applications, something that is evidenced by the large number of information security vendors who use it as part of their software development practices (Kay, 2005). TOGAF 9 ensures that as part of the architectural design of the IT infrastructure and supporting processes, the IT security
architecture is incorporated, thereby ensuring that all role-players throughout the organisation have a view of the blueprint of IT security (Pulkkinen, Naumenko & Luostarinen, 2007:1618).

What these frameworks discussed in this section have in common as a response to the IT risk themes is that they can be used to improve the software development practices of an organisation and consequently decrease software vulnerabilities. Therefore, none of these frameworks provide a direct response to the risk of hacking or the IT risk themes. But several control objectives are relevant by implication, such as integrity, accuracy, validity and security, due to the increased focus on quality during the software development process.

A balanced scorecard can be used to enable an organisation’s performance management system (ITGI, 2007a:11). A balanced scorecard can also be combined with other governance discipline, such as risk management. When defining controls for the identified risks, the metrics of a balanced scorecard can be defined to measure the effectiveness of the controls implemented. In doing so, the organisational IT objectives can be achieved (Kapur, 2010:47).

5.8.3 Dimensions of the quality management and software development responses

The software development and quality management standards discussed in this section are all process-oriented and do not define detailed control objectives or address IT risk themes at a technical level. The frameworks focus on improving software development practices, which may include a review of software security, before implementing the application in production, which focuses on mitigating the risk of hacking. The frameworks are therefore preventative in nature.

The only exception is the balanced scorecard, which can possibly be used to measure the effectiveness of the controls implemented to protect an organisation against hacker attacks. Since the measurement will take place after the event has taken place, it would be detective in nature.
5.8.4 Role-players in the quality management and software development responses

There are various role-players involved in the application of the frameworks discussed in this section. For the project management and system development frameworks, those would include typically project role-players, project managers, business analysts, software developers, testing coordinators, business stakeholders, business sponsors, end-users, project board, executives, senior suppliers of resources, and project assurance / auditors (PMI, 2008:222, 215, 246; Crown, 2009:13, 43, 269-272). From a quality management perspective, similar role-players from the project management office and the head of development will be involved (ITGI, 2007b:17). These role-players are not responsible for defining or implementing a response to hacking in general. Indirectly, by ensuring that secure software is developed, they could aid in the prevention of software vulnerabilities.

5.8.5 Advantages of the quality management and software development responses

Most of the frameworks discussed in this section might improve software development practices, which may lead to an increased ability to identify security vulnerabilities during software development, although it is not a specific focus of the frameworks. An advantage of the quality management framework ISO 9001 is that it will improve the overall software development process over time. An organisation will also be able to monitor and improve the software development process (Anderson, 2001:522).

5.8.6 Disadvantages of the quality management and software development responses

There are a number of complexities associated with quality management frameworks. ISO 9001 could be a superficial compliance process, with little substance (Anderson, 2001:522) and Six Sigma, which is not only expensive to implement but also requires statistical data and calculations for all possible process scenarios, requires specialist resources (Antony, 2008). This complicates the implementation and use of these frameworks, something that is exacerbated by the fact that the frameworks offer little value as a response to IT risk or hacking.

In the past, information security was often an afterthought in software development processes, with organisations following an ad-hoc process during software development to
ensure security is considered (Van Wyk & McGraw, 2005:75). More recently, there has been increased focus on including information security or software security into the software development processes (Nunes, Belchior & Albuquerque, 2010:48). Nonetheless, the software development and project management frameworks discussed in this section do not inherently include software security practices. When it is considered that they are best practice frameworks, the likelihood of developing software without considering security still exists. This is evident in the continued deployment of software with vulnerabilities and subsequent exploitation by hackers (as discussed in section 3.8.5).

5.8.7 Risks addressed by the quality management and software development responses

As part of the software development project activities, risks are identified which may affect the project’s objectives (Crown, 2009:81). Project risks are not necessarily applicable to the organisation as a whole.

Due to the software development focus of most of the frameworks discussed in this section, the IT risk themes addressed by these frameworks include inadequate change / project management practices, and data and application control weaknesses. Several of the control objectives can be relevant here from the perspective of including internal controls in the end-solution being developed.

5.8.8 Conclusion

Software development and quality management frameworks are essential in creating structure and discipline during software development projects. They apply only indirectly to the IT risk themes, including hacking, from the perspective of developing software with security in mind. This is however also a common weakness in software development frameworks, in that they have not been extended to include information security as a standard practice. System development and quality management provide a limited, incomplete response to the risk of hacking.

Thematological research questions

Based on the literature review above, the following thematological research questions can be defined:

IT Governance

- Whether there is a preference for any of the software development or quality management frameworks in
the banking sector.
  • The extent to which software development practices include information security design and development as a common practice in the banking sector.

**Hacking Response**
  • The extent to which software development practices include steps to improve the security of software and avoid software vulnerabilities in the banking sector.

### 5.9 HACKING AND THE INFORMATION SECURITY MANAGEMENT RESPONSE

#### 5.9.1 The essence of the information security management response

Organisations need to protect their most valuable assets, including data and information (Von Solms & Von Solms, 2005:271). Information security management enables the protection of these assets, as is evident in the definition of information security (Bidgoli, 2008:782-783):

> The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security.

Information security management is regarded as the ongoing operation and management of information security in an organisation (Nnolim, 2007:4; Amaio, 2009:8). The ultimate objective of information security management is to defend the information and the systems which produce the information from risks threatening their confidentiality, integrity and availability. The exchange of information between third parties and business partners through sophisticated communication channels needs to achieve the objectives of authenticity and non-repudiation (Information Systems Audit and Control Foundation, hereafter ISACF, 2001:9). Information security is enabled via the implementation of security controls, which include physical, technical and operational security controls (Posthumus & van Solms, 2004:642). It is submitted that information security management is enabled or supported in a number of ways, such as via best practice frameworks, information security governance, security configuration benchmarks or security technologies, which covers the broad range of physical, technical and operational security controls. Each of these will be discussed in turn, followed by the application of the response.
From a best practice framework perspective, ISO/IEC 17799:2005 (renumbered by the ISO to ISO/IEC 27002:2005) is one of the key global best practice frameworks in information security and a good starting point for defining a security policy document for an organisation (Calder, 2005:7; Van Niekerk, 2005:89; McGhie, 2006:181; Wright, 2008:112; ISO, 2008b). ISO 17799 provides control objectives and controls for 11 sections, which includes security policy; organisation of information security; asset management; human resources security; physical and environmental security; communications and operations management; access control; information systems acquisition, development and maintenance; information security incident management; business continuity management, and compliance (ISO/IEC, 2005:4; Kritzinger, 2006:46).

5.9.2 The information security governance response

Information security governance extends information security management by integrating it with an organisation’s corporate governance practices (Kritzinger, 2006:11; Nnolim, 2007:69). The ITGI (2006b:18) encapsulates this in the following definition:

Information security governance is a subset of enterprise governance that provides strategic direction, ensures that objectives are achieved, manages risks appropriately, uses organisational resources responsibly, and monitors the success or failure of the enterprise security programme.

Information security governance is essentially the way in which information security is deployed in the organisation to mitigate information security risks. It ensures appropriate human behaviour, cultivating a sense of responsibility for information security (Da Veiga & Eloff, 2007:361-362). Information security governance can be achieved for example by the application of comprehensive information security frameworks such as ISO 27002, alongside CobiT (Brotby, 2008:34, 35).

5.9.3 The security configuration benchmark response

Security configuration benchmarks are “used to denote sets of security configurations and settings that are recommended to achieve a specified level of security” (Fischer, 2005:40). Various organisations have developed security configuration benchmarks, such as the Center for Internet Security (hereafter CIS), NIST, Defence Information Systems Agency (hereafter DISA) and the National Security Agency (hereafter NSA) (Fischer, 2005:41).

For example, the CIS develops security configuration benchmarks and scoring tools, which
assist organisations in protecting themselves against common IT security vulnerabilities. Their tools are considered to contain best practice standards and are widely used by US government agencies and by auditors for measurement against ISO standards. They provide two levels of benchmarks: Level 1 being “the prudent level of minimum due care”, while Level 2 provides “prudent security beyond the minimum level” (CIS, 2009). It is important to note that their benchmarks are aimed at the technical configuration of mostly operating systems, network devices and firewalls (Wright, 2008:248).

5.9.4 The security technology response

From a security technology perspective, it is evident from security surveys that most organisations implement firewall or anti-virus software to mitigate the immediate risk posed by frequently occurring minor hacking and virus attacks (Richardson, 2008:18). Anti-spyware software could also be used to protect against minor hacking and spyware attacks (Anti-Spyware Coalition, 2006). An IDS and IPS are essentially more sophisticated extensions of firewall technology and could stop more complex hacker attacks (Bezuidenhout, 2002:146; Skoudis & Liston, 2006:320). Various technologies exist to manage the risk of unauthorised access to networks and applications, such as access control lists (hereafter ACLs), smartcards or tokens, biometric authentication, digital IDs and single sign-on functionality (Mapeka, 2000:148, 153; VeriSign, 2000; Anderson, 2001:27, 288; Newman, 2001; Khare, 2006:277, 281; Al-Azazi, 2008:100-101). To ensure the protection of an organisation’s data during transmission or storage, or to protect transactions with financial value, VPN, encryption or public key infrastructure (hereafter PKI) technologies could be deployed (Boshoff, 1998:31; Mapeka, 2000:163; Bezuidenhout, 2002:127; Khare, 2006:320, 338; Hitachi ID Systems, Inc. 2009).

5.9.5 Application of the information security management response

Similar to IT governance, information security governance incorporates information security management into the governance processes of an organisation. As data security is elevated to information security, it is further elevated to “business security”, to highlight the significance from a corporate governance perspective (Von Solms & Von Solms, 2005:272). Risks identified at an operational information security management level will consequently be reported at an information security governance level, bringing the risk of hacking to the attention of the board of directors. It remains mostly an indirect response, however, and needs to be augmented by a framework for a more detailed response.
ISO 17799’s target audience is those responsible for implementing or maintaining information security. It is used by organisations to benchmark their information security initiatives and monitor their maturity levels. It is also often used to achieve regulatory compliance, in particular where no guidance is provided in terms of information security expectations (McGhie, 2006:184; Kairab, 2006:1723). It does provide comprehensive information security controls and implementation guidelines and can be used as a baseline for information security. It is therefore a very direct response to selected IT risk themes and the risk of hacking. It is essential that IT management fulfils its information security duties, to ensure IT systems and applications are protected against hacker attacks. This responsibility is at times neglected, due to the focus on operational issues, rather than securing the IT infrastructure.

The CIS security configuration benchmarks are used by organisations to ensure compliance with requirements set by ISO standards and regulatory requirements specified by for example SOX and HIPAA (CIS, 2009). No doubt, IT management, internal auditors and ethical hackers can all make use of these benchmarks in their assessment of information security. These benchmarks can be used to mitigate some of the risks associated with hacking, most notably on a technical operating system level. More importantly, they will provide guidance on where the organisation should improve its internal processes, possibly making it more effective in identifying hacking events. The benchmark tool can also be used to ensure compliance with the organisation’s information security policies. It therefore provides a direct response to selected IT risk themes and the risk of hacking.

Technical security controls are most effective in their application against routine attacks from hackers and malware. It protects an organisation against the thousands of scanner tools and random exploits found and used by script kiddies (section 3.3.2) and cyber criminals. It also provides a direct response to selected IT risk themes and the risk of hacking.

5.9.6 Dimensions of the information security management response

As regards hacking from a risk versus event perspective, ISO 17799 recognises both, such as security events (ISO/IEC, 2005:23, 40, 55) and security risks (ISO/IEC, 2005:ix). The concepts “prevent” and “detect” are also comprehensively covered throughout the ISO 17799 text. Overall, ISO 17799 (and, by association, ISO 27002) provides comprehensive operational guidance on the management of hacker risks and events.

In the textbook “Handbook of Information Security Management”, used in preparation for the
CISSP exam, Tipton argues that information security controls can be divided into physical, technical and administrative controls, which can be either preventative or detective in nature (Tipton, 2006:210).

The security configuration benchmarks are mostly preventative in nature, since when applied, they will prevent hackers from exploiting system configuration weaknesses. Organisations implement preventative technical security controls, such as access control software, anti-virus software, passwords and encryption, to prevent unauthorised access to an organisation’s systems (Gurgul, 2004). Technical security controls are mostly preventative in nature, since they prevent attacks from succeeding and can be regarded as the first line of defence against hacker attacks.

Therefore, the information security management response is mostly preventative in nature, although it does consider detective controls as well. It covers the risk and event component of hacking.

5.9.7 Role-players in the information security management response

With the growing threat of cybercrime and the realisation of the vulnerability of information assets, the board of directors needs to be involved. Calder (2005:5-6) recognises the importance of the board of directors taking responsibility for information security. Information security governance facilitates this process (Cardholm, 2006:6). Information security governance ensures that information security role-players are included in existing risk committee forums, which leads to an increased focus on information security risks (Johnson, et al. 2009:51). Ultimately, information security governance should be the board of directors’ responsibility (Von Solms & von Solms, 2005:272). This could place the risk of hacking or at least the associated high-priority IT risk themes on the board of directors’ agenda. The responsibility for ensuring the information systems environment is secure also resides with the CEO and the executive management team (Crutchley, 2008).

Due to the significance of IT security risk and the need for information security governance, organisations started appointing CISOs (Whitten, 2008:15). The information security officer or CISO will be a key role-player at all levels of the information security management response, by setting the high-level policies and monitoring compliance against those policies. The CISO is also responsible for instilling a security culture (Johnson, Goetz & Pfleeger, 2009:45) in order to ensure that every employee plays a role in enforcing and complying with information security requirements, as well as being vigilant for suspicious
behaviour, such as insider activity. The CISO also plays a role in articulating the information security risks in a way that the board of directors will see it in the contexts of business risk, making it more palatable (Johnson, et al. 2009:48). The CISO or security executive often reports to the CIO, since the CIO approves the budget required for information security projects and initiatives (Johnson & Goetz, 2007:218). The CIO then also becomes a key role-player in enabling information security in an organisation.

5.9.8 Advantages of the information security management response

Information security reduces an organisation’s information security risk, while creating a secure environment in which to conduct business. The organisation benefits from an economic perspective, while supporting the achievement of its objectives (South African Centre for Information Security, hereafter SACFIS, 2010).

The benefits derived from implementing information security governance are encapsulated by Johnston and Hale (2009:127):

Because information security governance brings information security to the attention of Boards and CEOs, firms can more effectively and efficiently address the issue of information security leading to improved outcomes, including strategic alignment, risk management, business process assurance, and performance measurement.

When information security governance is combined with other frameworks, such as CobiT, and integrated with IT governance, it provides a wider response. Consequently, it can be used to address some of the risks forthcoming from the hacking threat. The focus is predominantly on securing business information and related systems, while obtaining the commitment from senior stakeholders in the organisation. When used as a response to hacking, greater awareness from the board and other senior stakeholders is achieved. This may lead to better funding and more specific focus on identifying the appropriate response to hacking.

Security configuration benchmarks ensure that an organisation achieves a minimum level of security, which could be in line with industry best practice when it makes use of the CIS benchmarks or other similar configuration benchmarks (Fischer, 2005:41). These benchmarks therefore provide a basic level of protection against certain hacker attacks.
5.9.9 Disadvantages of the information security management response

The challenges encountered in enabling information security management are captured in the following quote (Johnson, et al. 2009:49):

In the past, senior executives expected the CISO to ensure safety against viruses and hackers. However, many now realize that perfect security is unattainable, so the goal is risk mitigation, not risk elimination.

Although information security management is a highly applicable response to the risk of hacking, it cannot prevent every conceivable information security incident. Furthermore, increasing the information security knowledge in an organisation is regarded as challenging. Information security management is effective only when it is fully imbedded in all levels of the organisation (Johnson & Goetz, 2007:16-17). Information security governance does not provide a framework which addresses a wide range of IT risks. If not augmented by a best practice or framework, or not integrated with IT governance, it will provide a limited response to the threat of hacking.

There are some sceptics who believe that frameworks such as ISO 17799 do not always reduce information security risks (Johnson & Goetz, 2007:22). The focus of the ISO 17799 standard is predominantly on information security and does not cover the full scope of IT management responsibilities (ITGI, 2006a:28). It therefore has a limited and specific scope, although perhaps not as limited as some of the other responses discussed in this thesis.

Security configuration benchmarks tend to be very specific and limited in scope, since they focus on a particular operating system, network or database, without considering supporting processes (Fischer, 2005:41). It is unlikely that configuration gaps discovered during the application of security configuration benchmarks will be reported at a governance level. Therefore, although they provide a direct response to the threat of hacking, they do not provide a comprehensive response.

While organisations are increasingly investing in technical controls to protect themselves against hacker and virus attacks, they are realising that technical controls cannot be the only response to hacker attacks. In addition, technical security solutions, such as IPS and antivirus software, are not always effective in preventing hacker attacks (Waxer, 2008; Messmer, 2009). The unfortunate reality is that traditional technical preventative controls are not always effective in mitigating the risk of hacking. This is apparent in the following statement taken from the Information Security Breaches Survey 2010 (Infosecurity Europe &
More complex threats have emerged over the last two years. Technical controls are no longer, in isolation, enough to protect organisations. A combination of people, technology and process is now required.

Moreover, technical controls cannot, for example, protect against attacks from employees inside the organisation. Organisations then need to look at, for example, information security awareness training, to change the behaviour of employees (BERR, 2008:2).

5.9.10 Risks addressed by the information security management response

Information security management and information security governance do not define specific risks that could be addressed by the responses; however, arguably they would be risks threatening the primary control objectives of information security, which are confidentiality, availability and integrity of information.

The security configuration benchmark tools will assist in addressing the following IT risk themes, such as unauthorised logical access, cybercrime and possibly business and IT disruption, since the organisation’s system will be less vulnerable to an attack by hackers.

Through a literature review of the purpose and meaning of the security technologies, it is possible to indicate which IT risk themes could be covered by the security technologies (as reflected in Table 5.4). Similarly, it is possible to indicate which information security controls taken from ISO 27002 could be used as a response to the IT risk themes (also reflected in Table 5.4). There is comprehensive coverage of IT risk themes, although not every single IT risk theme has been addressed.

**Table 5.4 Security technologies and ISO 27002 as a response to the IT risk themes (own classification)**

<table>
<thead>
<tr>
<th>General controls:</th>
<th>Security Technologies</th>
<th>ISO 27002</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of compliance with IT policies and procedures, legal and regulatory requirements.</td>
<td>Penetration testing or vulnerability assessments to achieve compliance with security standards (ISO/IEC, 2005:104).</td>
<td></td>
</tr>
<tr>
<td>Business and IT disruption.</td>
<td>Anti-virus software, Firewalls / IDS / IPS</td>
<td></td>
</tr>
<tr>
<td>Inadequate IT operations and support.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Theft or damage to IT equipment.</td>
<td>Cabling security for equipment (ISO/IEC, 2005:34).</td>
<td></td>
</tr>
<tr>
<td>Inadequate change / project management</td>
<td>Applications and operating systems should</td>
<td></td>
</tr>
<tr>
<td>Issue</td>
<td>Controls</td>
<td>Countermeasures</td>
</tr>
<tr>
<td>-------</td>
<td>----------</td>
<td>-----------------</td>
</tr>
</tbody>
</table>

**Application controls:**

- **Application control weaknesses.**
  - Web / URL filtering, Smartcards / Tokens, Digital ID, Single Sign-on

- **Data control weaknesses.**
  - Encryption, Smartcards / Tokens, Public key infrastructure (PKI), Digital ID, Single Sign-on
  - Secure handling of media, including the disposal of end-of-life media (ISO/IEC, 2005:46, 47).

- **Interface / network control weaknesses.**
  - Firewalls / IDS / IPS, Encryption, Access control list (ACL), Smartcards / Tokens, Public key infrastructure (PKI), Digital ID, Single Sign-on

- **Operating system weaknesses.**
  - Anti-virus software, Firewalls / IDS / IPS, Access control list (ACL), Smartcards / Tokens, Digital ID, Single Sign-on
5.9.11 Conclusion

The information security management response can be applied in a number of ways. The information security governance response could ensure that information risks are classified as business risks and appropriately treated. The use of best practice frameworks, such as ISO 17799, provides a more detailed response to the threats posed by hacking, although it is not a detailed response to business or IT risks in general. It is comprehensive in providing a response to information security risks, but does not cover all the IT risk themes. The use of technical configuration benchmarks and security technologies provides a lower-level response to the threats posed by hackers, but such benchmarks and technologies are generally limited in scope and do not elevate the threat to a corporate governance level. Perhaps a combination of all of the information security management responses is required to provide an effective response.

Although information security management provides a more comprehensive response to the IT risk themes and hacking than other responses, it does not provide a fully comprehensive response.

<table>
<thead>
<tr>
<th>Thematological research questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Based on the literature review above, the following thematological research questions can be defined:</td>
</tr>
</tbody>
</table>

Corporate Governance

- The extent to which information security management is addressed in the banking sector.
- Whether information security management has been integrated into corporate governance policies, procedures and the culture within the banking sector.
- Determining who is responsible for information security management in the banking sector.
- Whether the information systems and controls of the banking sector incorporates to the control objectives.
- Whether there is a fundamental understanding of the concept “information security governance” in the banking sector.
- Whether there is awareness in the banking sector of information security governance and the role it can play.
- Whether information security governance is addressed in any way in the banking sector.
- The scope of information security governance in the banking sector and whether ethical hacking is included, towards achievement of information security goals.
- The extent to which security technology solutions are integrated into information security management, ERM and IT governance processes in the banking sector.
- The extent to which results achieved through security technology solutions are reported at board level in the banking sector.

IT Governance

- Whether information security management is embedded within the IT governance practices of the banking sector.
Hacking Response

- Whether information security management is considered as a response to the threat of hacking in the banking sector.
- The extent to which information security governance is used as a response to hacking in the banking sector.
- The extent to which information security management frameworks such as ISO 27002 are used as a response to hacking in the banking sector.
- The extent to which technology solutions are applied in the banking sector to address the risk of hacking.
- To determine which suite of technology solutions are applied in the banking sector.
- The extent to which security technologies are effective in responding to or mitigating hacker attacks in the banking sector.
- The extent to which there is an understanding in the banking sector, that technology solutions cannot be the only response against hacker attacks.

5.10 CHAPTER SUMMARY

As part of a comprehensive literature study, chapter 4 identified that there is a strong link between the business risks defined by King II (supported by risk management principles in King III) and a generic set of pervasive IT risks and control objectives. Furthermore, the link between the business risks, IT risks and hacking was established. It has led to the conclusion that the effect of hacking is pervasive throughout the organisation.

This chapter has explored a number of responses to the threat of hacking. It was argued that the various possible responses are not equally effective in addressing the threat of hacking. In essence, some responses are indirect in nature, whereas others provide only a partial or incomplete response. In a few instances, a comprehensive response is provided, but perhaps it is not in-depth enough to mitigate the risk of hacking at a granular level.

The corporate governance and risk management responses provide only an indirect response to the hacking threat. Although significant from a governance perspective to ensure the focused attention by the board of directors, they do not provide a direct response. ERM does have its advantages in that it might assist in the identification of the pervasive risk of hacking, while formulating an integrated response. But, risk management processes often exclude detailed risks, such as hacking. Also, only a few organisations have effectively implemented ERM.

In itself, IT governance provides only an indirect response to the threat of hacking, closely integrating it with corporate governance and ensuring IT objectives align with business objectives. When combined with a framework, such as CobiT 5, a comprehensive response is achieved.
A partial or incomplete response is provided by a number of responses, such as the IT service management, quality management, project management, software development, and security configuration benchmark responses. These are only effective in addressing some of the IT risk themes, but are not effective in providing a comprehensive response against the hacking threat.

The most comprehensive responses provided to the IT risk themes were internal control, the two frameworks CobiT 5 and ISO 27002 and lastly security technologies. The two frameworks ensure integration with the IT governance and information security management responses, whereas internal control provides a very direct response. Internal control is a requirement of good corporate governance and cannot be ignored in the formulation of the ultimate response against hacking. Security technologies provide the least comprehensive response. To illustrate the coverage of the IT risk themes identified in chapter 4, the most comprehensive frameworks identified in this chapter are mapped against the IT risk themes. The results are summarised in Table 5.5.

Table 5.5 Summary of the comprehensive responses to the IT risk themes (own summary)

<table>
<thead>
<tr>
<th>General controls</th>
<th>Internal control</th>
<th>CobiT 5</th>
<th>Security Technologies</th>
<th>ISO 27002</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorised physical access / lack of physical access control and security.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Lack of compliance with IT policies and procedures, legal and regulatory requirements.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Business and IT disruption.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Inadequate IT operations and support.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Theft or damage to IT equipment.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Inadequate change / project management practices.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Misuse of IT / irregularities and fraud.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Cybercrime.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Inadequate IT performance.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Complexity of IT.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inefficient use of IT resources.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT human resource deficiencies.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application control weaknesses.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Data control weaknesses.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Interface / network control weaknesses.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Operating system weaknesses.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Lack of an audit trail.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lack of segregation of duties.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Internal control as a response has a fundamental weakness, in that it can be circumvented. It is therefore not always effective as a response. Although CobiT 5 provides good coverage of the IT risk themes, the response is mostly defined at a process level and lacks granular
detail. It is apparent that none of the frameworks provide a perfect or fully comprehensive response to the IT risk themes. It follows that these frameworks will not provide a comprehensive response to the threat of hacking.

In general, there is good coverage from the comprehensive responses identified in this chapter of the control objectives, with a slight bias towards the control objectives confidentiality, integrity and availability. Perhaps this is not surprising, since corporate governance and IT governance recognise the importance of information security, where these three control objectives dominate.

Even the most comprehensive response to the IT risk themes does not provide an infallible response to the threat of hacking. The inherent nature of hacking is such that it circumvents the responses and controls meant to prevent the threat. The hacking threat also keeps on evolving and adapting to new technologies, possibly rendering the responses discussed in this chapter ineffective. The controls implemented to protect against the hacker threat need to be assessed to determine whether they are effective enough against the hacker threat. It is from this perspective that a further, and perhaps more effective, response to hacking will be considered: ethical hacking.
CHAPTER 6

The ethical hacking response

6.1 INTRODUCTION

The significance of the hacking threat has repeatedly been highlighted in previous chapters. It could affect each business risk, leading to business disruption, financial and/or reputational losses. Hackers could circumvent controls meant to protect an organisation. Chapter 5 reflected on the range of responses that are available to address the threat of hacking. These responses can range from overall corporate governance to technology solutions. It has also been highlighted that these responses are not always effective in addressing the risk of hacking. One of the most important responses in the context of this thesis is the use of ethical hacking. This chapter will focus on ethical hacking as an in-depth comprehensive response to the threat of hacking.

Firstly, the origin and meaning of ethical hacking and ethical hackers will be explored. Next, this chapter will profile ethical hackers. Then a generic ethical hacking methodology is presented, followed by the clarification of terms synonymous with ethical hacking. This chapter then goes on to discuss the placement of ethical hackers in an organisation and the skills requirements and qualifications of ethical hackers. The need for ethical hacking is explored, followed by the application of ethical hacking and how it augments some of the responses identified in chapter 5. The advantages and disadvantages of ethical hacking are also considered, and this is followed by the dimensions of the ethical hacking response. Role-players in the ethical hacking response are discussed briefly. This chapter will also discuss ethical hacking as a response to the business risks, IT risks themes and control objectives identified in this thesis, to illustrate the comprehensiveness of the ethical hacking response.

6.2 THE ORIGIN AND MEANING OF ETHICAL HACKING AND ETHICAL HACKERS

6.2.1 Introduction

Ethical hacking is at times considered a controversial practice (Higgins, 2009), with the
concept of justifying “breaking into” and possibly disrupting an organisation’s network and systems not finding favour with every business executive or system owner. It might be that these perceptions are misguided, due to a lack of understanding the concept “ethical hacking”.

Ethical hacking is not a new concept, yet not a common practice followed in all organisations. Moreover, at times there is a misunderstanding of what exactly ethical hacking entails and how it relates to the crime of hacking (Gupta, 2011a): “A lot of people don’t understand the difference between hacking and ethical hacking.” This section will provide clarity on this concept and related terminology.

### 6.2.2 Historical origins of the terms “ethical hacking” and “ethical hacker” in brief

The origins of ethical hacking are not clear. Some believe that ethical hacking originated in the US military in 1974 when the US Air Force conducted realistic tests on their Multics operating system (Palmer, 2001a:770). Others believe that the first example of penetration testing dates back to 1975, as explained in a paper entitled “Operating System Penetration” by Linde (Smith, Yurcik & Doss, 2002:377, 379). Others believe that it originated from a paper published in 1993 on UseNet, entitled “Improving the security of your site by breaking into it”, by Dan Farmer and Wietse Venema, authors of one of the earliest hacker tools, SATAN (Security Analysis Tool for Auditing Networks). Farmer and Venema emphasised one of the underlying objectives of ethical hacking, which is to enable system administrators to understand how their system can be compromised (Farmer & Venema, 1993:2; Computer Weekly, 2008b). Yet others are of the opinion that ethical hacking found its origin in the information security field (Saleem, 2006:201) when the need arose to test an organisation’s IT systems, which in itself created a niche business opportunity, as information security specialists or “ethical hackers” provided their specialised skills for hire (Schell & Martin, 2004:2).

### 6.2.3 Defining “ethical hacking”

Regardless of the precise origins of ethical hacking, there are a host of definitions found in the literature that describe its nature. Beaver (2004:11) encapsulates the essence of ethical hacking in the following statement:

To catch a thief, think like a thief. That’s the basis for ethical hacking.
He goes on to state that (Beaver, 2007a:11):

Ethical hacking – which encompasses formal and methodical penetration testing, white-hat hacking, and vulnerability testing – involves the same tools, tricks, and techniques that hackers use, but with one major difference: Ethical hacking is legal because it’s performed with the target’s permission.

Another definition focuses on the controversial nature of ethical hacking (Livermore, 2007:111):

Ethical hacking is the controversial practice of employing the tools and tactics of hackers to test the security precautions protecting a network.

The EC-Council defines ethical hacking as (EC-Council, 2008a:32) follows:

Ethical hacking is broadly defined as the methodology that ethical hackers adopt to discover existing vulnerabilities in information systems’ operating environments.

Three possible reasons for conducting ethical hacking assignments could be (Ross, 2001:11-12):

- To find obvious weaknesses in the security of the network or operating systems of organisations.
- To find vulnerabilities in software applications that could be exploited by a hacker.
- To test comprehensively those systems that are critical for the organisation.

The need for ethical hacking is also driven from a legal or regulatory perspective. In the US, vulnerability assessments or penetration testing assessments are a mandatory legal requirement for the following legislation or security standards: Payment Card Industry (hereafter PCI) Data Security Standard; HIPAA legislation and the GLBA (Oppleman, et al. 2005:247; Khare, 2006:186; PCI Security Standards Council, 2006:12; Core Security Technologies, 2007; Ohwobete, 2009:200, 301).

When ethical hacking is defined, the multi-faceted nature of ethical hacking should be recognised, as should the broad range of areas it could potentially cover (Corsaire Limited, 2007):

- Commercial products, such as operating systems and databases.
- Custom applications, such as web-applications.
- Telephony, such as war-dialling.
- Wireless technology.
• Employees, through social engineering.
• Physical, such as a review of access controls and dumpster diving.

Due to the nature of ethical hacking, there are inherent risks associated with the activity. However, it is possible to manage an ethical hacking assignment in such a way that the “resulting damage is predictable and repairable” (Knight, 2009:39). Graves (2007:7) argues that hacking can be ethical. According to Graves, the key is to exclude the destructive component of hacking and to understand the legal liabilities associated with ethical hacking activity.

Therefore, ethical hacking may be regarded as the process of using the same tools, mindset and techniques a hacker would use in gaining access to a system, with the primary difference being that he or she does it with legal intent and with the target’s permission. It is a process of uncovering security weaknesses and active attacks against the target (Smith, et al. 2002:374; Holt, 2005:52; Fried, 2006: 408, 409; Graves, 2007:7, 8; Mansfield-Devine, 2009:12; Bavisi, 2010:263). It is regarded as an activity with a wider scope than penetration testing, and would include testing techniques, such as social engineering (Knight, 2009:39).

6.2.4 Defining “ethical hackers”

Various complementary views on the meaning of ethical hacking are found in the literature. Graves (2007:7) typifies ethical hackers as “usually security professionals or network penetration testers who use hacking skills and toolsets for defensive and protective purposes”. Ethical hackers are also defined as independent security professionals attempting to break into a computer system or to identify security vulnerabilities (Palmer, 2001a:770; Matusitz, 2006:282). The keyword is “attempt”, since the objective is not necessarily to break into, damage the system or steal information. Instead, the ethical hacker would report to the client on the vulnerabilities discovered and how they could be remedied (EC-Council, 2002:2). It should be noted that they can work either for independent information security consultants or external audit firms, but may also be employed internally in an organisation (Schleifer, 2006).

Ethical hackers employed by an organisation hack into their own organisation, or more simply put, rigorously test their own network security. They discover the vulnerabilities and weaknesses before hackers can exploit them. The organisation tests the effectiveness and robustness of its security measures (Fried, 2006:409; Darragh, 2009:124). Closely linked to the definitions of ethical hacking, the EC-Council defines ethical hackers as (EC-Council, as
The goal of the ethical hacker is to help the organisation take pre-emptive measures against malicious attacks by attacking the system himself; all the while staying within legal limits.

Similar to a hacker, the ethical hacker will try to determine what useable information can be obtained from the target system. A hacker would use the information for personal benefit or to advance the attack. In contrast, the ethical hacker will use the information to protect and defend the organisation (Graves, 2007:7, 8). Ethical hackers are regarded as trustworthy (Sholomyansky, 2007:12), and will only “hack” into a system to test the security. Ethical hackers are creative in nature, with the ability to find unexpected security flaws. They also need to be determined and patient in finding elusive vulnerabilities (Geer & Harthone, 2002:189, 190). Ethical hackers have to specialise in the art of penetration testing. The higher their level of specialisation, the more likely that they will find vulnerabilities (Geer & Harthorne, 2002:185).

A hacker would use his skills and techniques for “illegal intent”, whereas an ethical hacker would use them to identify security vulnerabilities, therefore with “legal intent” (EC-Council, 2008a:33). It can be compared with a locksmith, who would lock-pick a car door, not to steal it, but to let the owner in. Therefore, a locksmith practises his profession with “legal intent”.

Beaver (2004:14) argues that an ethical hacker has to abide by three basic rules:

- The ethical hacker should uphold the highest ethical principles at all times. An ethical hacker has no hidden agendas and supports an organisation’s overall goals.
- All information collected during an assignment should be kept private. Passwords should not be used to access confidential corporate information.
- The ethical hacker should not deliberately (or accidentally) crash the system being tested. The ethical hacker can avoid this by fully understanding the system being exploited and the tools used to carry out the test.

It is submitted that the word “ethical” adds significant contexts to the term “ethical hacker”, and underpins the nature of ethical hacking activity.
6.2.5 Conclusion

Although the exact origin of ethical hacking is unclear, it has become a recognised testing technique in the information security industry. Ethical hackers make use of the same tools and techniques used by their malicious counterpart, hackers. A significant difference, however, is that ethical hacking is conducted with the target's permission.

<table>
<thead>
<tr>
<th>Thematological research questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Based on the literature review above, the following thematological research questions can be defined:</td>
</tr>
</tbody>
</table>

**Hacking Response**
- The extent to which ethical hacking is regarded as an acceptable practice or profession in the banking sector.
- The extent to which the concept ethical hacking and the objectives of ethical hacking are understood in the banking sector.
- The extent to which it is understood in the banking sector that ethical hackers uphold the highest ethical principles.

**IT risk**
- Whether the banking sector realises that ethical hacking can be managed in such a way that the risk is minimised.

6.3 ETHICAL HACKER PROFILES

6.3.1 Introduction

To understand the nuances of “ethical hacking” and “ethical hackers”, the profiles of ethical hackers need to be considered. These profiles provide further insight into the activities of ethical hacking. Three profiles will be discussed: white hat hackers, tiger teams and red teaming.

6.3.2 White hat hackers

The profile “white hat hacker” has already been discussed extensively in section 3.3.6. Suffice it to say here that white hat hackers are also at times classified as ethical hackers.

It is important to note, however, that a distinction between white hat hackers and ethical hackers is noted in the literature. White hat hackers can work anonymously, without
expecting compensation for their discovery of software vulnerabilities. Ethical hackers, or perhaps rather “security professionals”, would be contracted or employed by an organisation to find security vulnerabilities (Duke, 2002:3; Holt, 2005:183). This distinction is important, since ethical hackers might be more trustworthy, due to their educational background or affiliation with professional institutions. White hat hackers might have obtained their “practical” skills from hacking into organisational systems to test their skills. The converse might also be true, in that white hat hackers might be more skilled, due to their practical skills (Duke, 2002:3; Holt, 2005:183) or due to their dedication and almost “scientific” approach towards identifying vulnerabilities and truly understanding how a system can be attacked (Schultz, 2002:383). As discussed in section 3.3.6, a white hat hacker's motives might be slightly questionable. From ethical hackers working in a professional capacity, only the highest ethical values would be expected.

Hacker profiles can be positioned according to skills level and ethical viewpoint. Ethical hackers by implication have very high moral ethical values and their average skills levels could be placed at an intermediate level. To expand on Figure 3.1: ethical hackers can be closely positioned with white hat hackers, as depicted in Figure 6.1. It is submitted that an ethical hacker’s skill level might be slightly lower compared to the typical position of a white hat hacker, seeing that a white hat hacker might have more practical experience. It is also not unlikely, for ethical hackers to be less skilled, but more morally just when compared to white hat hackers. As in Figure 3.1, the positions are relative, and not definitive, which implies that an ethical hacker could potentially have über hacker skills.

Figure 6.1  Comparing ethical hackers with other hacker profiles (own deduction)
6.3.3 Tiger teams: A synonym for an ethical hacker group

A group of ethical hackers are sometimes referred to as a “tiger team” (Palmer, 2001a:770) and ethical hacking as “tiger testing”. Tiger testing therefore refers to the ethical hacker task of finding all unknown security vulnerabilities, which is performed by a group of ethical hackers. Consequently, this is where the distinction is found between ethical hackers and black hat hackers. Black hat hackers have to find only one exploitable security vulnerability in order to break into a system.

Often, an ethical hacker has to find all possible vulnerabilities and recommend remedial action. It is submitted that the ethical hackers who are part of a tiger team would have similar objectives (such as securing the organisation’s system) and therefore similar ethical viewpoints.

6.3.4 Red teaming

Ethical hacking is also referred to as “red teaming”, where ethical hackers do extensive tests to detect all possible vulnerabilities (Peake, 2003:1; Wright, 2008:5). A red team can be seen as a team of ethical hackers conducting penetration testing.

Wright (2008:5) defines red teaming as follows:

Red Teaming differs from penetration testing in that it is designed to compromise or penetrate a site at all costs. It is not limited to any particular attack vector (such as a VPN or Internet) but rather is an attempt to access the system in any feasible manner (including physical access).

Red teaming assignments are often conducted by external audit firms or information security specialists. They often use commercial vulnerability assessment tools during their assignments. One of the major drawbacks of these assignments is the cost and prolonged test timeframe (Cohen, 1998; Samant, 2011:11-12). The term “red team” was taken from the military, where the so-called “good guys” are the “blue forces” and the “enemy” is called the “red team”. This process involves the simulation of black hat hackers. The red team will attack the network from an unknown point and remain hidden during the engagement (Harris, et al. 2005:81; Gallegos & Smith, 2006:51). The “blue team” testing will occur when the organisation’s IT staff are fully informed of the test. The drawback with this approach is that the IT staff could prepare for the attack and consequently this does not simulate the real-life situation of hacker attack (Wack, Tracy & Souppaya, 2003:3-12; Samant, 2011:11).

A blue team can also work in collaboration with a red team, where the red team focuses on
finding technical vulnerabilities, whereas the blue team focuses on providing advice on how to mitigate the potential exploitation of these vulnerabilities from a process or IT governance perspective (Veerasamy, 2009:1).

A red team could also include an auditor alongside ethical hackers or information security specialists. This is particularly useful where “red teeming” is done as part of an assurance engagement or as part of addressing information security practices. The auditor would also benefit from this kind of assessment through knowledge sharing (Gallegos & Smith, 2006:53).

6.3.5 Conclusion

The profiles white hat hackers, tiger teams and red teaming in essence refer to the same role-players: ethical hackers. The profiles are indicative of the scope of the ethical hacking assignment, where both tiger teams and red teaming focus primarily on vulnerability assessments and white hat hackers would most likely conduct penetration testing. The similarity between the profiles and ethical hacking in general is depicted in Figure 6.2.

Figure 6.2 Synonyms for ethical hackers and ethical hacking (own presentation adapted from Krutz & Vines, 2001:472 & Fletcher, 2007)

Now that the hacker profiles have been explored, a generic ethical hacking methodology will be defined and each methodology stage discussed.

Thematological research questions

Based on the literature review above, the following thematological research questions can be defined:

**Ethical Hacking**
- The extent to which the banking sector recognises the difference between ethical hackers and white hat hackers.
6.4 ETHICAL HACKING METHODOLOGY

6.4.1 Introduction

The ethical hacking process is a systematic process of analysing IT security weaknesses. The best way of conducting a systematic review is to follow a formal methodology to ensure consistency and avoid oversights (Khare, 2006:193-194).

The intention is never to follow the methodology to the letter, but rather to use it as a general guideline to ensure that all significant steps have been completed. In ethical hacking, there is always a level of creativity. This characteristic ensures that ethical hackers find undiscovered vulnerabilities. The generic methodology might also have to be adjusted, depending on the type of assignment (Oppleman, et al. 2005:232-233; Khare, 2006:193).

6.4.2 Towards a general ethical hacking methodology

There is no single definitive ethical hacking methodology. However, there are numerous similarities between the ethical hacking methodologies presented in hacking and ethical hacking sources. A number of methodologies discussed in the literature will be outlined here.

Firstly, Skoudis and Liston (2006:183-668) defined five phases typically followed during a hacking or ethical hacking assignment:

- Phase 1: Reconnaissance.
- Phase 2: Scanning.
- Phase 3: Gaining access and DoS attacks.
- Phase 4: Maintaining access.
- Phase 5: Covering tracks and hiding.

Secondly, Oppleman, et al. (2005: 233-235) defined the following phases:

- Information gathering / reconnaissance.
- Mapping out your theatre of war.
• Target qualification.
• Attack profiling.
• Attacking.

Thirdly, Scambray and McClure (2003: xxvi), authors of the popular “Hacking Exposed” series, have defined the following phases:
• Footprint.
• Scan.
• Enumerate.
• Penetrate.
• Escalate.
• Get interactive.
• Pillage.
• Expand influence.
• Clean up.

Fourthly, Tiller (2005:38) defined the following phases to be followed by an ethical hacker when penetration testing is conducted, while the business implications are also considered:
• Planning.
• Operations.
• Reconnaissance.
• Enumeration.
• Vulnerability analysis.
• Exploitation.
• Final analysis.
• Deliverable.
• Integration.

Harris, et al. (2005:78-98) defined the following ethical hacking methodology phases:
• Assessment planning.
• Discovery.
• Vulnerability enumeration.
• Exploiting mapped vulnerabilities.
• Reporting.

Beaver (2004:29, 41-51, 299) set out the following ethical hacking phases:
• Developing your ethical hacking plan.
• Gathering public information.
• Mapping the network.
• Scanning systems.
• Assessing vulnerabilities.
• Penetrating the system.
• Reporting your results.

Next, Day (2003:186-192) defined nine steps to be followed when ethical hacking is engaged in:

• Step 1: Audit preparation.
• Step 2: Object discovery.
• Step 3: Risk assessment.
• Step 4: Vulnerability scanning.
• Step 5: Hands-on audit.
• Step 6: Hands-on sampling.
• Step 7: Physical inspection.
• Step 8: Compiling and scoring data.
• Step 9: Reporting and review.

Young and Aitel (2004:57-58) defined the following phases:

• Reconnaissance.
• Mapping targets.
• System / network penetration.
• Denial-of-service.
• Consolidation.
• Security.

Next, Deloitte (Deloitte & Touche, 2002:15-35) defined the following four phases as part of their penetration testing and vulnerability services:

• Phase 1: Initiating an attack and penetration engagement.
• Phase 2: Information gathering and targeting techniques.
• Phase 3: Enumeration.
• Phase 4: Vulnerability assessment and exploitation.

Also, Earle (2006:228-233) defined the following phases:
• Information gathering.
• Enumeration.
• Compromise.
• Expand privileges and accessibility.
• Cleaning up the trails.

Graves (2007:5-6), author of the official CEH review guide, defined the following phases:
• Phase 1: Passive and active reconnaissance.
• Phase 2. Scanning.
• Phase 3: Gaining access.
• Phase 4: Maintaining access.
• Phase 5: Covering tracks.

Following this, the Information Systems Security Assessment Framework defines the following multi-layered phases (Open Information Systems Security Group, 2006:128):
• Phase I: Planning and preparation.
• Phase II: Assessment.
  o Information gathering.
  o Network mapping.
  o Vulnerability identification.
  o Penetration.
  o Gaining access & privilege escalation, enumerating further, compromise remote users / sites, maintaining access, covering tracks.
• Phase III: Reporting, clean-up and destroy artefacts.

Finally, the Penetration Testing Framework 0.5, authored by Orrey (2008a), defines the following phases:
• Pre-inspection.
• Network footprinting.
• Discovery and probing.
• Enumeration.
• Password cracking.
• Vulnerability assessment.
• Penetration.
• Final report.
From the above, it is clear that none of the methodologies listed are exactly the same. At the same time, all of them share at least one or more similar methodology phases. Consequently, for the purposes of this thesis, the following generic phases for ethical hacking have been identified:

- Preparation.
- Footprinting.
- Scanning.
- Enumeration.
- Vulnerability assessment.
- Exploitation.
- Maintenance.
- Recommendation.

For the discussion of the generic methodology, it would be assumed than an ethical hacker or red team would conduct the assignment. Each of these phases will be discussed in turn.

### 6.4.3 Preparation phase

One of the most critical tasks during the preparation phase is to obtain approval for the ethical hacking assignment. Approval should be obtained from the system owner or an executive, who could support the ethical hacker should something go awry during the assignment. The approval should always be in writing to protect the ethical hacker from possible legal action. This is also referred to as a liability release (Fried, 2006:409; Tittel, et al. 2003:48; Beaver, 2004:29-30; Graves, 2007:206; Bavisi, 2010:263). Authorisation for conducting the ethical hacking assessment should be obtained from the highest role-player in the organisation possible (Van den Berg, 2009).

An ethical hacker may be asked to sign a nondisclosure agreement, should he or she come across confidential information during the assignment (Graves, 2007:206). The assignment carried out by an ethical hacker should be classified and the necessary security measures should be in place to ensure that confidential information obtained during the assessment remains secure (Sholomyansky, 2007:12; Van den Berg, 2009). An ethical hacker might even have to go as far as signing a legal document, granting the ethical hacker permission to conduct the ethical hacking assignment (Leathers, 2008:13). While ethical hackers use the same tools and techniques as hackers, common sense prevails, in that some techniques would be illegal. For example, ethical hackers should not bribe the target organisation’s
employees for sensitive information to assist them in hacking into the organisation. Information gathering should only be conducted in the public domain (Van den Berg, 2009).

During the preparation phase, the goal of the ethical hacking assignment should be clearly defined, since this will allow the ethical hacker to determine whether the outcome of the assignment is a success or failure (Fried, 2006:409). The specific objectives and goals of the ethical hacking assignment have to be documented. It needs to be specified whether the ethical hacker should obtain confidential data, execute a business application, change a system configuration or only provide proof that access was obtained (Bishop, 2007:84). Further objectives and goals are documented in Table 6.1.

Table 6.1 Ethical hacking objectives, rules and goals (Beaver, 2004:30-36; Saleem, 2006:202; Knight, 2009:40; Trull, 2012:23)

| − Start and finish dates of the assignment, as well as the scope and depth of testing. |
| − Timing of the testing, such as during peak or non-peak processing hours. |
| − Prioritising the items to be tested, through focusing on the vulnerabilities that have a high likelihood of being attacked. |
| − The specific target and technology to be tested. |
| − Whether the client will be notified or whether a “real-life” test will be conducted without notifying the client (covert vs. overt). |
| − Defining the expected outcome and how legal ramifications will be dealt with. |
| − Defining the tests to be conducted (e.g. penetration testing, password cracking or war dialling). |
| − Whether the assessment will be conducted from the internal network or whether it will be conducted externally (e.g. an Internet café). |
| − Tests to be performed on the test or production platforms. |
| − The tools to be used during the assignment: Safe tools which won’t affect the system or any tool that a hacker would use to gain access. |
| − How service disruption can be prevented when attacks affect the target systems. |

To ensure consistency when conducting penetration testing, the use of checklists might assist with ensuring all common vulnerabilities are found. Creating network and application diagrams might provide greater clarity towards achieving the intended objectives (Chapela, 2010:6, 7).

The decision as to whether the assignment should be conducted externally or internally to the organisation is an important consideration. During an external assessment, the likelihood of hacker attacks is assessed. The organisation’s perimeter defences (such as firewalls and IDSs) are tested to determine whether they will withstand hacker attacks. During internal assessments, the likelihood that an insider will obtain access to the organisation’s systems will be assessed. In this scenario, the ethical hacker will have authorised physical access. There would be a focus on logical access controls and social engineering (Brancik, 2005:67-69). More value might be attained by defining business objectives, as opposed to technical objectives when planning penetration testing. For example, the objective should be to hack
into a particular business system, as opposed to breaking into the organisation in general (Chapela, 2010:6).

6.4.4 Footprinting phase

During the footprinting stage, general public information about the target / organisation is collected. This is referred to as “passive reconnaissance”, since information relevant to the target organisation will be collected without its knowledge. It has a similar objective to hacker’s reconnaissance phase. The primary source for public information is the Internet. Through general and specific Web engine searches, a considerable amount of detail can be obtained, for example: employee names, job experience and contact info, press releases on organisational changes and new products. Information regarding IT infrastructure being used by the organisation could also be collected, for example the type of firewall implemented. Dumpster diving and social engineering are other techniques used to obtain general information (Internet Security Systems, Inc. 2000:52; Young & Aitel, 2004:60; Beaver, 2004:41, 42; Earle, 2006:228; Parker, 2007:5; Basta & Halton, 2008:19; Orrey, 2008a).

Also during the footprinting stage, the target network can be mapped by making use of public databases and resources available via the Internet. Search engines can be used to find a wealth of information on the target company (Earle, 2006:229; Basta & Halton, 2008:28-29). This is done to determine the address range of the target network. This is used in particular when conducting a “black box” external assignment, as discussed in section 6.5.2. This information is required during later stages of the ethical hacking process (Graves, 2007:27).

6.4.5 Scanning phase

During the scanning phase, the ethical hacker may conduct one or more of the following activities: scanning, fingerprinting and banner grabbing. Each will be discussed in turn.

Firstly, the scanning activity involves scanning for active hosts, modems and open ports. The first step would be to identify live hosts on a network. This is often done via a ping sweep of the IP address range. Once all live hosts have been discovered, a port scan will be conducted to identify available services on each live host. A popular tool used for detecting active hosts is SuperScan, and one of the best tools to detect open ports is NMap (Beaver, 2004:46; Graves, 2007:43-45; Samant, 2011:13, 27). One of the most commonly used wireless scanners is Network Stumbler (Earle, 2006:294). A “host” is any computer with full
two-way access to other computers on the Internet. It could also be a computer running a web server, hosting one or more Web sites. A “web server” is software running on a host computer connected to the Internet, configured to respond to HTTP requests from other web browsers (Khare, 2006:300, 339). Open ports are scanned in order to detect applications running on those ports: for example, TCP port 21 might be showing that an FTP service is running (Khare, 2006:48).

Secondly, another process conducted during the scanning phase is “fingerprinting”. Fingerprinting involves the process of identifying vulnerable hosts, such as through identifying the operating system.

Thirdly, “banner grabbing” is used to connect to an open service to read and interpret the information returned. Often, enough general information is returned to allow the identification of the particular service software and operating system used on the target system (Young & Aitel, 2004:80; Graves, 2007:52).

### 6.4.6 Enumeration phase

Enumeration involves the process of gathering usernames, machine names, network resources, shares and services. It is a process of actively connecting to the target system in order to obtain this information. The user account and system account information obtained could be used during the exploitation phase to gain access into the system (Graves, 2007:55-56; Basta & Halton, 2008:31). Two examples of enumeration approaches are presented.

Firstly, one of the most successful ways of obtaining user credentials is through social engineering techniques (Schell & Martin, 2004:54):

- Glancing over an authorised user’s shoulder when he or she is in the process of logging in.
- Recording the user’s keystrokes on video.
- Looking for clues on the user’s desk.
- Calling the system administrators (as opposed to the helpdesk) and claiming to be an employee who forgot his password.
- Searching through the rubbish for user credentials.
- Guessing combinations of initials and birth dates of authorised users.
Secondly, all network infrastructure devices such as routers and switches include simple network management protocol (hereafter SNMP) agents, which are used to manage those devices. The agents are often left with the default usernames and passwords, which are easily obtainable from the web. Hackers may use these devices to advance or perform an attack (Graves, 2007:58).

### 6.4.7 Vulnerability assessment phase

During the vulnerability assessment stage, the ethical hacker will identify and assess vulnerabilities in the target system. These vulnerabilities can be assessed manually, which may be very time consuming, or through automated tools. There are various commercial vulnerability assessment tools available, which are easy to use and give excellent summary reports. Open source vulnerability assessment tools, such as SARA, might also be considered (Internet Security Systems, Inc. 2000:132; Beaver, 2004:50; Graves, 2007:207; Tutakhail, 2010:28). Although automated vulnerability assessment tools produce results in a significantly shorter timeframe, caution must be taken in not accepting the results at face value. The ethical hacker will have to analyse and validate the results. Human intelligence is always a key factor in ethical hacking assignments (Oppleman, et al. 2005:240).

It is important to note that up to this point in the methodology, the likelihood of a material negative effect on the target systems, due to the ethical hacking activity performed, is low, when carefully planned and executed. In the next phase, the likelihood of material negative impact on the target system is high.

### 6.4.8 Exploitation phase

The objective of the exploitation phase is to break into the system. Two approaches may be followed: password cracking and exploiting vulnerable services. Once access has been obtained, the hacker will escalate his privileges.

Firstly, a common technique used to break into a system is password cracking. Users often choose passwords that are easy to remember. The ethical hacker would attempt to guess the passwords for valid user accounts. Manual password cracking is not very efficient; therefore automated scripts and tools are often used to test a comprehensive list of passwords. The most efficient way of password cracking is to obtain the password file from the system and use a tool, for example John the Ripper, to decipher the password hashes. A password hash is the encrypted format of the clear text password (Graves, 2007:68).
Password hashes could be obtained by monitoring or sniffing the traffic to and from the target system. Once the hash is obtained, a password cracking tool could be used to decrypt it. A more direct approach is to use an automated tool, which passes usernames and passwords to the authentication mechanism (Young & Aitel, 2004:90). Secondly, a hacker might decide to break into the system via an exploit. To be successful in breaking into a target, the ethical hacker has to find a vulnerability that is exploitable. It may be possible to find exploit code (small pieces of software code written in programming languages, for example, C) for those vulnerabilities in underground Web sites or on IRC channels (Earle, 2006:231; Samant, 2011:14).

The ethical hacker would avoid certain hacking attack types, which may disrupt normal business processes, such as man-in-the-middle attacks and buffer-overflow exploits (Chapela, 2010:7). During the exploitation stage, the ethical hacker may perform any number of actions, for example:

- Start or stop services or applications.
- Access other systems from the target.
- Capture screen shots (of current actions) or upload a file as proof of breaking into the target (Beaver, 2004:51).

There are freeware tools available that automate exploitation. A good example is the Metasploit framework, which contains a number of ready-to-use exploits, which could be used to break into a target system (Oppleman, et al. 2005:246; Graves, 2007:140; Tutakhail, 2010:30).

During this stage, a further important point from a hacker perspective is the escalation of privileges. This is often done by taking advantage of flaws in the system that will allow the hacker to escalate his privileges (Earle, 2006:231). Privileges are escalated in order to be able to carry out more powerful actions on the compromised system. The intention is to gain access to the system and propagate from one system to another, until a whole network segment has been “conquered”. Root or administrator privileges will be obtained in the operating system, providing the ethical hacker with full control over the system (Harris, et al. 2005: 10; Brancik, 2005:66-67; Graves, 2007:204). An ethical hacker would indicate in the original scope of his assignment whether exploitation would include the need to prove that escalation of privileges would be possible.

It is important to note that the exploitation phase of the methodology is the controversial
phase of an ethical hacking assignment, in that the action carried out during the exploitation phase could possibly affect the target system.

6.4.9 Maintenance phase

Similar to a hacker, the ethical hacker would maintain the access obtained, in particular when the ethical hacking assignment consists of multiple phases, where multiple targets must be breached.

During this phase, the ethical hacker would disable auditing tools to ensure that malicious actions are not logged (Graves, 2007:85). The ethical hacker would delete logs files containing evidence of his actions. This is to avoid being detected by the system administrators (Earle, 2006:233; Graves, 2007:86). Backdoors could be installed to allow the ethical hacker to gain easy access back into the compromised system (Earle, 2006:231; Graves, 2007:92). Again, these are sensitive actions, which need prior approval from the system owner. The ethical hacker can decide not to engage in maintenance activities.

6.4.10 Recommendation phase

During the recommendation stage, the ethical hacker will document the results of the ethical hacking assignment. The report will include details of the scope of the test, for example, whether it was a vulnerability assessment or penetration test. The report will also include general details of the network or systems tested during the assignment. The ethical hacker may have to include a non-technical executive summary for non-IT literate business executives (Orrey, 2008b). Beaver (Willey Publishing, Inc. 2006) makes a critical statement, when discussing the reporting phase of ethical hacking, by pointing out that the ethical hacker should report all vulnerabilities discovered and not only a selected few. This reflects on the honesty of the ethical hacker. The ethical hacker should also report high-risk vulnerabilities immediately to management, to allow the organisation to correct these as soon as possible. It might be worthwhile combining the results with a risk rating in order to prioritise the vulnerabilities. The final report should include details of the assignment, when the tests were conducted and recommendations of how to correct the vulnerabilities. Due to the sensitive nature of the ethical hacking report, it is critical that the document is marked as confidential and delivered securely to trustworthy individuals, on a “need-to-know” basis. This is to avoid a malicious user from obtaining the information to perpetrate a crime (Beaver, 2004:299-304; Oppleman, et al. 2005:252; Samant, 2011:14-15).
Graves (2007:208) provides suggestions on the following items to be included in the final report:

- Findings listed in descending risk priority order.
- An analysis, conclusion and remediation measure defined for each finding.
- Supporting evidence, for example log files.
- Executive summary of the organisation’s security profile.
- Name of the ethical hacker and when the test was conducted.
- Any positive comments regarding the organisation’s security posture.

6.4.11 Conclusion

This section identified a generic ethical hacking methodology, based on a literature study conducted. The objective of each phase is summarised below:

- **Preparation:** Completing the logistics before commencing with the ethical hacking assignment, such as obtaining approval and determine the scope.
- **Footprinting:** General information on the target is collected from public sources.
- **Scanning:** The organisation’s network environment is scanned for active hosts and open ports.
- **Enumeration:** More specific details are obtained from the active hosts, such as usernames and machine names.
- **Vulnerability assessment:** By means of vulnerability assessment tools, security vulnerabilities and security flaws are identified on the target systems.
- **Exploitation:** By means of password cracking or exploiting vulnerable services and applications, access is obtained into the target system.
- **Maintenance:** Once access has been obtained, the ethical hacker has to delete activity logs, to ensure he or she remains undetected.
- **Recommendation:** On completion of the ethical hacking assignment, the ethical hacker will compile a report with all his observations (vulnerabilities identified) and recommendations for remediation.

Now that the generic ethical hacking methodology has been discussed, it is possible to explore terms that are synonymous with ethical hacking, since an understanding of the generic methodology aids in distinguishing between the different terms.
Thematological research questions

Based on the literature review above, the following thematological research questions can be defined:

**Ethical Hacking**
- Whether an ethical hacking methodology is used when conducting ethical hacking within the banking sector.
- Whether each phase of the generic ethical methodology is executed in the banking sector.
- Whether the ethical hacker obtains explicit consent for conducting ethical hacking assignments in the banking sector.
- To determine how the banking sector deals with confidential information disclosed during ethical hacking assignments.
- Whether ethical hacking assignments are conducted by disclosing them to management or by conducting them without notifying management in the banking sector.
- Whether the goals and objectives on an ethical hacking assignment are clearly defined in the banking sector.
- To determine whether the banking sector sets boundaries for ethical hacking assignments.
- Whether the overall results of ethical hacking assignments reach the board of directors in the banking sector, or whether only operational management receives the results.
- Whether the results of ethical hacking assignments are understood by the board of directors in the banking sector.
- Whether the report of an ethical hacker contains only selected vulnerabilities or all the vulnerabilities identified.
- Whether both internally and externally executed ethical hacking assignments are conducted in the banking sector.
- Whether ethical hacking assignments are scheduled to take place during non-critical business hours in the banking sector.
- Whether the banking sector allows the use of freeware tools during ethical hacking assignments.
- Whether there is management oversight of ethical hacking activities in the banking sector.
- To determine whether the banking sector conducts social engineering assignments and what the outcome of those assignments are.
- Whether the banking sector makes use of commercial or open source tools during vulnerability assessments.
- Whether certain hacker attack types are prohibited during ethical hacking assignments by the banking sector.
- Whether the banking sector conducts regular scans of their network environment, in order to detect unnecessary open ports and unsecured wireless networks.
- Whether the banking sector is aware of the kind of information that can be obtained via footprinting (passive reconnaissance) and social engineering.

**Business risk**
- Whether ethical hacking assignments are considered a risk in the banking sector.
- To determine how the risks associated with ethical hacking assignments are managed in the banking sector.

**IT risk**
- Whether the banking sector is aware of the risks associated with the exploitation phase of ethical hacking methodology.
6.5 EXPLORING TERMS SYNONYMOUS WITH ETHICAL HACKING

In the information security industry, there are several terms used synonymously with the term ethical hacking, such as penetration testing, white-hat hacking, security testing or attack and penetration studies (MIS Corporate Defence Solutions Ltd., 2000:6; Brandt & Vines, 2001; Graves, 2007:6; Beaver, 2004:10; Beaver, 2007a:11; Schell & Martin, 2004:2; Landoll, 2006:20; Hartley, 2006:3; Computer Weekly, 2008a; Khan, 2010:15). Most often, penetration testing is used as synonym for ethical hacking (Pathak, 2005:145; McAdam, 2007:3). It is important though to acknowledge that there are differences between the various terms. Simmons (2008:1) is of the opinion that “penetration testing" is a more accurate description of the activity being conducted, compared to the use of the term “ethical hacking”. However, like the word “cracker”, which is a more accurate description of a malicious hacker (as discussed in section 3.3.3), the term has not been widely accepted in the media or information security industry. It would rather seem that the term “ethical hacking” has been accepted by organisations as the descriptive label and individuals offering ethical hacking services (BBC Tyne, 2008), referring to a broader testing approach when compared to penetration testing (Knight, 2009:39). However, there are important differences and similarities between the two terms “ethical hacking" and “penetration testing" and the closely related term “vulnerability assessment”, which will be explored in this section.

6.5.1 Vulnerability assessment

Beaver defines vulnerability assessments as the process of identifying security vulnerabilities in the organisation’s systems. He defines the following characteristics associated with vulnerability assessments (Beaver, 2007b):

- More detailed and structured when compared to a penetration test.
- The assessment is not necessarily restricted to a single target. The scope might extend to a large or total component of the organisation’s network, databases and systems.
- Many ethical hacking tools are required to identify all possible vulnerabilities.
- Vulnerability assessment approach is not limited to automated vulnerability assessment scanning (typically done with commercial tools), but includes manual assessment techniques as well.

Wright (2008:6) defines a vulnerability assessment as follows:

A vulnerability assessment is an assessment and gap analysis of a site’s or a
A vulnerability assessment is a risk-based process. The process involves the identification and classification of primary vulnerabilities that may result in a system impact.

Peltier, Peltier and Blackley (2003:4-5) argue that vulnerability assessments have two primary goals. The first goal is to test everything. The objective is to identify all vulnerabilities. There is however a time and cost dimension associated with such an exercise. This may affect the ability to identify all possible vulnerabilities (depending on the approach, such as manual versus automated vulnerability assessments). Vulnerabilities could be identified individually by the ethical hacker, but this may be a daunting task, since there are thousands of potential combinations of tests that need to be performed in order to discover all weaknesses in an operating system. The easier route would be to make use of an automated tool (Harris, et al. 2005: 9).

The second goal highlighted by Peltier, et al. (2003:4-5) is to provide management with a useful report, which can be used to inform them of the most critical issues. Information collated during the vulnerability assessment exercise will be collated into meaningful information. The vulnerability assessment tool also assists with ranking the severity of the risks or vulnerabilities identified. Furthermore, some of the aspects reported by vulnerability assessment tools include software versions, software patches, open ports and deviations from the companies’ security policies. Vulnerability scanners often provide guidance on how to fix certain vulnerabilities (Wack, et al. 2003:3-3; Heikkila, 2009:4, 5, 20).

Vulnerability assessment tools often report “false positives”. A “false positive” is where a vulnerability assessment tool reports a weakness, which on closer investigation turns out to be incorrect or non-existent (Wright, 2005; Landoll, 2006:20). This is due to the thousands of configuration possibilities in operating systems or applications. Another drawback of vulnerability assessment scanning is that it may generate additional network traffic, which may have an adverse effect on the target systems (Wack, et al. 2003:3-4). Vulnerability assessment tools also only highlight known software security vulnerabilities (Khan, 2010:16). There still might be many undiscovered software vulnerabilities.

As regards the phases of the generic ethical hacking methodology, a vulnerability assessment assignment would not engage in the phases, exploitation and maintenance (as depicted in Table 6.2), since the objective is only to identify vulnerabilities and not to exploit the vulnerabilities. The ethical hacker would focus on earlier stages, since possible targets have to be identified. The ethical hacker would also publish the results of vulnerabilities
discovered during the recommendation stage.

<table>
<thead>
<tr>
<th>Stages of an ethical hacking process</th>
<th>Vulnerability Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preparation</td>
<td>Yes</td>
</tr>
<tr>
<td>Footprinting</td>
<td>Yes</td>
</tr>
<tr>
<td>Scanning</td>
<td>Yes</td>
</tr>
<tr>
<td>Enumeration</td>
<td>Yes</td>
</tr>
<tr>
<td>Vulnerability Assessment</td>
<td>Yes</td>
</tr>
<tr>
<td>Exploitation</td>
<td>No</td>
</tr>
<tr>
<td>Maintenance</td>
<td>No</td>
</tr>
<tr>
<td>Recommendation</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Generally speaking, though, vulnerability assessment assignments can be seen as a softer or safer approach to follow during ethical hacking assignments.

6.5.2 Penetration testing

Penetration testing goes further than only identifying security vulnerabilities (Voogt, Roos & Van der Watt, 2008:9). Fried defines it as follows (Fried, 2006:408):

Penetration testing is defined as a formalized set of procedures designed to bypass the security controls of a system or organization for the purpose of testing that system or organization’s resistance to such an attack. Penetration testing is performed to uncover the security weaknesses of a system and to determine the ways in which the system can be compromised by a potential attacker.

Bianco sees penetration testing as a control mechanism. He defines penetration testing as follows (Bianco, 2006:426):

Penetration testing involves examining the security of systems and architectures. It reviews the effectiveness of the security of the organization’s Internet presence. This includes all the holes and information that might damage the organization. The tester uses his creativity and resourcefulness to behave in the same manner as a hacker would.

Wright (2008:4) defines it as follows:

A Penetration test is an attempt to bypass controls and gain access to a single system. The goal of the Penetration test is to prove that the system may be compromised.
Beaver defines penetration testing as follows (Beaver, 2007b):

A penetration test looks through the eyes of a malicious attacker to determine which vulnerabilities – typically in externally-facing systems – can be exploited and what level of access can be gained.

Although, generally, penetration testing is associated with hacking into a system, the literature outlines that the scope of penetration testing could include many facets, such as vulnerability scanning, ad-hoc testing, war dialling and social engineering. It is often conducted by an independent team, with the aim of testing the effectiveness of the organisation's controls against external attacks (Landoll, 2006:20; Evans, 2009:12). A particular objective of penetration testing is to perform a "detailed analysis of the threats and potential attackers" (Bishop, 2007:84). This implies that the ethical hacker should be familiar with the various hacker profiles (discussed in section 3.3) and objectives of hackers, as well as the possible motives behind their attacks, as discussed in section 3.5.

When compared to other security assessment approaches, which may follow a rudimentary checklist approach, penetration testing takes a more hands-on approach (Corsaire Limited, 2007). It is seen as a means of “assuring information security”, with assurance provider objectives of adequate coverage (Computer Weekly, 2008b). It is also regarded as an “informal non-rigorous technique for checking the security of a system” (Engle, 2010:2-3). Penetration testing can also be seen as an extension of vulnerability assessments, where the vulnerabilities discovered during vulnerability assessments are exploited during penetration testing (Wu, 2007:40). Penetration testing can also specifically focus on exploitation of weaknesses and obtaining actual evidence of data that could be stolen, to highlight the significance of the breach. It can be scoped to focus on breaching the system, rather than identifying all possible vulnerabilities (Trull, 2012:21).

Beaver describes the following characteristics associated with penetration testing (Beaver, 2007b):

- The scope of the assessment is clearly defined, with a specific target in mind.
- The process is less structured than a vulnerability assessment.
- It requires a high level of technical skill.
- A smaller number of ethical hacker tools are required than the number used during vulnerability assessments.
- Testing may include social engineering.
- It only covers Internet facing systems.
The term “penetration testing” is used synonymously with the term “ethical hacking” (Xiong & Peyton, 2010:174; Pietro & Verde, 2010:16). Penetration testing comprises the full generic ethical hacking methodology (reflected in Table 6.3). In particular the exploitation and maintenance phases are included in this type of assessment.

Table 6.3 Ethical hacking stages covered by penetration testing (own deduction)

<table>
<thead>
<tr>
<th>Stages of an ethical hacking process</th>
<th>Penetration Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preparation</td>
<td>Yes</td>
</tr>
<tr>
<td>Footprinting</td>
<td>Yes</td>
</tr>
<tr>
<td>Scanning</td>
<td>Yes</td>
</tr>
<tr>
<td>Enumeration</td>
<td>Yes</td>
</tr>
<tr>
<td>Vulnerability Assessment</td>
<td>Yes</td>
</tr>
<tr>
<td>Exploitation</td>
<td>Yes</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Yes</td>
</tr>
<tr>
<td>Recommendation</td>
<td>Yes</td>
</tr>
</tbody>
</table>

From the discussion above, the following similarities with the concept ethical hacking is evident. Like ethical hacking:

- Penetration testing also involves the use of hacking tools and techniques.
- Penetration testing is conducted via a formal process and can also be viewed as an information security methodology.
- Penetration testing is used to identify security vulnerabilities and information security weaknesses in an organisation’s defences.

The term “penetration testing” is often used to refer to assignments that actually involve breaking into the system and generally can only be done by highly skilled individuals, in order to minimise the potential negative effect on the target system (Wack, et al. 2003:3-11; Trull, 2012:21, 23). During penetration testing, the ethical hacker will test the vulnerabilities discovered during the vulnerability assessment process. Effectively, then, the vulnerability assessment is followed by penetration testing (Harris, et al. 2005: 10; Brancik, 2005:66-67; Graves, 2007:204).


- **Black box model** – The ethical hacker has limited knowledge of the network. Only a few people within the organisation are notified. This model is very similar to a real black hat hacker breaking into an unfamiliar organisation.
• **White box model** – The ethical hacker will have a lot of information available about the network and organisation. This includes access to employees within the organisation. The scope of the assignment might be more specific and the assignment could be completed in less time compared with a “black box” assignment.

• **Grey box model** – This would involve a hybrid approach between the black box and white box model. The ethical hacker, acting as a “black hat” hacker, would solicit information from the “insider” to plan and launch his attack.

The organisation will have to decide which approach holds the most value for it. A black-box approach may provide information on how black hat hackers could gain access to a system, whereas the white-box approach may focus more specifically on weaknesses in for example, the network perimeter (EC-Council, 2008a:51). It is important to note at this point of the discussion that ethical hacking assignments do not imply by default that the ethical hacker will break into the system. However, the term “penetration testing” is associated with breaking into the target system. The action of breaking into the target system is not malicious in nature. The ethical hacker should know when to stop a penetration test, before real damage is done (Saleem, 2006:202).

### 6.5.3 Vulnerability assessment versus penetration testing

Beaver (2007b) is of the opinion that ethical hacking covers both penetration testing and vulnerability assessments. Some ethical hacking vendors will offer the choice of either a vulnerability assessment or penetration testing, or even both. When both services are requested, penetration testing will be preceded by some form of vulnerability assessment. It is also often followed by remediation of information security weaknesses found (eWeek, 2007). In order to break into a system, security vulnerabilities need to be identified first. This approach is similar to the ethical hacking methodology, which was presented in section 6.4.

Given that both vulnerability assessment and penetration testing approaches are used in the generic ethical hacking methodology, it follows that ethical hacking assignments could be scoped to be either a vulnerability assessment assignment or a penetration testing assignment. The two options can be seen as “two levels of intensity” (Voogt, et al. 2008:9). The difference in scope is important, since this allows the ethical hacker to choose either a more conservative or slightly more “aggressive” approach to ethical hacking.

Vulnerability assessments and penetration testing can both be classified as ethical hacking. Vulnerability assessment involves only the identification of potential vulnerabilities in the
target system. Penetration testing, on the other hand, includes actually gaining entry via the vulnerabilities into the target network or system. The disadvantages of a vulnerability assessment assignment is that the ethical hacker only identifies potential vulnerabilities, whereas penetrating testing provides more convincing evidence of actual weakness in the target’s security. This is done through validation of the actual vulnerability, by testing it. The disadvantage of a penetration test is that it may cause disruption to network services or production systems (Oppleman, et al. 2005:245; Graves, 2007:204).

The difference between vulnerability assessments and penetration testing is clearly stated by Oppleman, et al. (2005:246):

Vulnerability assessments evaluate a system in hopes of finding suspected vulnerabilities, whereas pen testing verifies suspected vulnerabilities by actually attempting to exploit them.

The only real difference between the two types of assessments is that vulnerability assessment assignments exclude the generic ethical hacking phases of exploitation and maintenance (reflected in Table 6.4).

<table>
<thead>
<tr>
<th>Table 6.4 Vulnerability assessment versus penetration testing (own deduction)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stages of an ethical hacking process</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Preparation</td>
</tr>
<tr>
<td>Footprinting</td>
</tr>
<tr>
<td>Scanning</td>
</tr>
<tr>
<td>Enumeration</td>
</tr>
<tr>
<td>Vulnerability Assessment</td>
</tr>
<tr>
<td>Exploitation</td>
</tr>
<tr>
<td>Maintenance</td>
</tr>
<tr>
<td>Recommendation</td>
</tr>
</tbody>
</table>

Beaver (Willey Publishing, Inc. 2006) makes an important statement when discussing the two approaches. He points out that a penetration test will have a limited scope in terms of the target being assessed. The objective is to breach the organisation’s security, whereas vulnerability assessments focus on identifying all possible vulnerabilities. The objective is to remediate all vulnerabilities present in the organisation’s systems. Penetration testing is closely associated with the exploitation phase of ethical hacking (breaking into the system). The terminology is also descriptive in its meaning, hence the reason for using it as a synonym for ethical hacking. Since the two approaches, vulnerability assessment and penetration testing, present two different levels of scope and intensity, the concepts are consequently more indicative of the test approach to be followed during an ethical hacking.
A distinct difference between hacking and ethical hacking exists. Hacking focuses more on the latter phases of the generic methodology (discussed in section 3.6) – that is, breaking into or exploiting the system (which is after all the primary objective of a hacker: to break into the organisation’s systems) – whereas ethical hacking tends to focus more on the former phases of the generic methodology: planning and assessment phases (an ethical hacker wishes to highlight all the vulnerabilities, not only prove that it is possible to break into the organisation’s systems).

It is submitted that the difference between vulnerability assessment assignments and penetration testing assignments is crucial in the context of this thesis. An important theme that will be addressed in the fieldwork is management’s reluctance to approve an ethical hacking assignment with a full “penetration testing” scope. Management might be more willing to approve an ethical hacking assignment with a “vulnerability assessment” scope, which is less obtrusive.

It is important to note that for the remainder of this chapter, the terminologies “penetration testing” or “vulnerability assessment” refer to ethical hacking in general, while at the same time maintaining their individual meanings.

6.5.4 Conclusion

Vulnerability assessment and penetration testing are terms used synonymously with the term ethical hacking. Vulnerability assessment focuses on comprehensively identifying all possible vulnerabilities within an organisation, whereas penetration testing focuses on providing proof that it is possible to break into an organisation. These two testing approaches can be used to scope an ethical hacking assignment.

An important consideration in the use of ethical hacking is deciding on the best placement of ethical hackers, either internal or external to an organisation.

<table>
<thead>
<tr>
<th>Thematological research questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Based on the literature review above, the following thematological research questions can be defined:</td>
</tr>
<tr>
<td><strong>Hacking Response</strong></td>
</tr>
<tr>
<td>• Whether the banking sector prefer to conduct vulnerability assessment or penetration testing.</td>
</tr>
</tbody>
</table>
6.6 THE PLACEMENT OF ETHICAL HACKERS

One of the most contentious issues associated with ethical hacking is the placement of ethical hackers. Since the literature lacks clear direction as to the best placement of ethical hackers, what follows in this section is merely a listing of some of the viewpoints. Essentially, ethical hackers can be placed either internally (permanent employment) or externally (third party services) to an organisation. It is submitted that there are a great many factors to be considered in the decision to place ethical hackers internally. These include the frequency of attack by hackers and cybercriminals; the complexity and criticality of the IT environment; the lack of focus on information security; non-disclosure of the organisation’s security posture; and high susceptibility to social engineering, although very few of these are specifically highlighted in the literature.

Internally placed ethical hackers might be more familiar with the organisation’s network and application environment, and even software development practices, giving them an advantage in finding vulnerabilities (Geer & Harthorne, 2002:191). It is submitted that other factors ethical hackers should be familiar with include the risk profile of the organisation, competency and skill of internal staff, perimeter security devices and how they are managed. In-house ethical hackers might also be considered when there is a high degree of sensitivity associated with the applications being developed or a high degree of confidentiality associated with the information that may be exposed (Geer & Harthorne, 2002:191). An internally placed ethical hacker may be used to collaborate in in-house investigations when insider hacking activity is suspected (Norfolk, 2001:7).

There could also be other determining factors for placing an ethical hacker internally. The cost of ethical hacking assignments could be more expensive when external providers, who tend to be more specialised, are used (Geer & Harthorne, 2002:191). An organisation’s IT staff may benefit greatly from the knowledge shared by internally placed ethical hackers, which could lead to improving information security in general and ensuring that security
technologies are securely configured, such as firewalls (Norfolk, 2001:7).

When appointing an ethical hacker to be placed internally, a thorough background check should be carried out, in order to determine whether the ethical hacker has not engaged in illegal activity in the past. It is imperative that the character and social viewpoints of ethical hackers are assessed in order to determine their moral viewpoints (Duke, 2002:3; Pepose, 2006:A02). The absence of a criminal record seems to be a preferred hiring test between white hat hackers and ethical hackers (Jagnarine, 2005:13). The practice of hiring ex-hackers remains controversial (Gupta, 2011b). Psychometric testing should also be considered, to determine the individual’s values (Van den Berg, 2009). An alternative would be to hire (or “headhunt”) an ethical hacker from a reputable company, such as one of the audit firms, which often have ethical hacking teams (Lyman, 2002). To ensure the ethical hacker’s independence and objectivity, he or she might even be placed in internal audit. In smaller organisations, an ethical hacker might report to the CFO or the designated information security officer (Padayachi & Keyser, 2008). From a corporate governance and King III perspective, the CIO will be tasked with managing IT, which includes the responsibility to secure the corporate information (IoD, 2009b:84, 86). It is argued that an ethical hacker might therefore be placed inside the CIO’s organisational structure, to assist with information security management responsibilities. Sanders (2006:3) argues that strong security skills have become paramount for IT specialists. This includes not only a theoretical base, but also practical experience in managing information security. Consequently, organisations employ ethical hackers in their IT department to find vulnerabilities and information security weaknesses (Lyman, 2002; Schleifer, 2006). Ethical hacking could be a lucrative career option, with companies offering up to a £100,000 annual salary for qualified ethical hackers (Hoare, 2006). Within a South African context, CEH-qualified ethical hackers are paid up to a R714,000 annual salary (PayScale, Inc. 2011).

White hat hackers have sometimes acquired their skills through illegal means. An organisation therefore might unknowingly appoint an “ethical hacker” with a criminal past (Edwards, 2007). When placing an ethical hacker, the hiring organisation could insist on ethical hacking certification as a means of confirming the ethical hacker’s skill and ethical viewpoint. Ethical hackers might also be respected in the security industry, since well-respected ethical hackers are often asked to present at security conferences (Leung, 2005). During the recruitment of an ethical hacker, the hacker in question should be able to demonstrate that he or she has (Bhattacharyya & Alisherov, 2009:3):

- An above average understanding of IT and other ethical hacking knowledge areas, such as open source tools and operating systems.
• The ability to write clear reports and explain technical aspects to a “non-technical audience”.
• Good customer relationship skills.
• A minimum of two years of ethical hacking experience.
• A clear understanding of the legal issues associated with ethical hacking.

Externally placed or “outsourced” ethical hackers have the advantage of being objective in their assessments and have often attained a higher level of specialisation than ethical hackers placed inside an organisation. Externally placed penetration testers might also have the ability to complete an ethical hacking assignment in less time and more comprehensively than in-house ethical hackers. Due to the short turnaround time, there could be cost benefits as well (Geer & Harthorne, 2002:190, 191; Jagnarine, 2005:14; Wu, 2007:41). A disadvantage associated with externally placed ethical hackers is that their history of hacking activity might be unknown. Externally placed ethical hackers may also overstate the risk associated with a particular vulnerability, to extend their services provided, rather than providing a true reflection of the security stance of the organisation (Norfolk, 2001:7). To protect the organisation, background checks will have to be conducted on the ethical hackers from service providers (Brancik, 2005:492), unless the service provider offer professional indemnity. The cost of third party ethical hacking service providers could also be more expensive (Geer & Harthorne, 2002:191).

Ethical hacking assignments are often conducted by an independent outside firm that specialises in ethical hacking (or penetration testing) specifically, such as SensePost (Pty) Ltd. (hereafter SensePost) and TelSpace (SensePost, 2011a; Telspace Systems, 2011). It is argued that they have the time and resources to specialise in the development and use of ethical hacking tools. They will also have an independent view on the security of the organisation, since they are not familiar with the internal workings of the organisation’s networks or systems. As a result of their independence, full disclosure of all security weaknesses is also more likely (Krutz & Vines, 2001:473; Tittel, et al. 2003:48). They often conduct black-box testing, with limited insight into the organisation’s security measures. Audit firms also offer ethical hacking services; however, the scope of their assignments is often limited to vulnerability assessments only, as opposed to physically hacking into the system (Rodger, 2000), even when relying on professional indemnity, due to the risks associated with penetration testing. To ensure that the confidentiality and security of ethical hacking assignments conducted by an outside firm are maintained, the following attributes should be achieved (PwC, 2000):
• The consultants should make use of a structured methodology, aimed at preventing system downtime and loss of data.
• Consultants will undergo background checks, to ensure their integrity during assignments.
• The consultants should be technically competent and understand the latest hacking techniques and tools.
• The consultants should have several years of experience working in the industry, alongside a clear understanding that the risk appetite of each industry varies.

The ethical hacking service provider should also be able to demonstrate the following (Bhattacharyya & Alisherov, 2009:3-4):
• Ethical hacking is an essential part of its business.
• Several years of industry experience.
• Independent research and contribution to the security community.
• Background and qualifications of testers.
• Their policy in relation to the confidentiality of data.
• References from other clients.
• Insurance cover to protect the client.

In larger organisations, external ethical hacking services are sometimes requested by internal audit departments or security divisions, as a means of providing an additional level of assurance or highlighting issues that might be still outstanding from the defined audit scope. In smaller organisations, the CEO, CFO or Chief Operating Officer (hereafter COO) might be asking for ethical hacking services, as a concrete means of providing a view on the security posture of the organisation. There may also be a need for independent assessment, to provide the CEO, CFO or COO an insider view of whether the security posture is really in order, in particular when there is a “no, everything is under control” syndrome present among IT support staff (Van den Berg, 2009). Where applicable, the CEO delegates his IT responsibilities to the CIO (IoD, 2009b:84). Also, as argued earlier in this section, the CIO might also have to consider the use of ethical hackers, due to his responsibility towards information security. Finally, a hybrid approach might provide the ideal results, where external penetration testers work in collaboration with a technical specialist inside the organisation to identify the most likely areas where vulnerabilities may exist (Geer & Harthorne, 2002:191).

As part of the placement criteria, an ethical hacker might be required to have a formal
qualification. The general skills requirements and well known ethical hacking qualifications will be discussed next.

<table>
<thead>
<tr>
<th>Theoretical research questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Based on the literature review above, the following thematological research questions can be defined:</td>
</tr>
<tr>
<td><strong>Ethical Hacking</strong></td>
</tr>
<tr>
<td>• The extent to which the banking sector comprehends the differences between internally and externally placed ethical hackers.</td>
</tr>
<tr>
<td><strong>Hacking Response</strong></td>
</tr>
<tr>
<td>• Whether the banking sector makes use of internally or externally placed ethical hackers.</td>
</tr>
<tr>
<td>• Whether special recruitment practices are considered when appointing ethical hackers in the banking sector.</td>
</tr>
</tbody>
</table>

### 6.7 SKILLS REQUIREMENTS AND QUALIFICATIONS FOR ETHICAL HACKERS

It is an unwritten prerequisite for an ethical hacker or penetration tester to be technically proficient, beyond mere general IT knowledge (Geer & Harthorne, 2002:189). Ethical hackers generally have an above average understanding of operating systems (for example Windows, Unix and Linux), networks, programming and related technologies (PrepLogic, Inc. 2007:5; Graves, 2007:10). Ethical hackers apply the same tools and techniques as black hat hackers, albeit with a positive intention (Harris, *et al.* 2005:8-9; Pipkin, 1997:5, 11). Ethical hackers require practical knowledge of penetration testing tools, such as software proxies, vulnerability scanners, fuzzers (automated bug finding through repeated data injection), port scanners and sniffers. Over and above these, they would also know how to use normal web browsers and debuggers (used to test and debug programs) to their advantage (Geer & Harthorne, 2002:190). The ability to write programs in programming languages, such as C++ and Perl would be an advantage (Fletcher, 2007), but is not essential, given the significant number of hacker tools available. Nonetheless, they often have extensive experience in developing software. It is not unusual for penetration testers to develop their own hacking tools (Geer & Harthorne, 2002:189, 190). In order to protect an organisation against hacker attacks, an ethical hacker needs to understand how these attacks are undertaken. Ethical hackers independently review the target system’s security and report the vulnerabilities discovered to management (Graves, 2007:10). They should also be familiar with risk management and incident response practices, to help an organisation recover from successful hacking attempts (Saleem, 2006:202) or even the outcome of an ethical hacking assignment, which might have affected the system.
As would be the case for hackers, ethical hackers have to continuously up-skill and expand their knowledge (Beaver, 2004:11). They have to stay abreast of the latest techniques applied by the hacker community. One way of achieving this goal is by attending conferences and seminars on hacking, such as the Black Hat Briefings held annually in Las Vegas (Wilbanks, 2008).

Several institutions offer ethical hacking training, such as SensePost (2011b), which offers hands-on beginner to advanced hacker training. Examples of official certification offered by the SysAdmin Audit Network Security (hereafter SANS) Institute (The SANS Institute, 2011a; The SANS Institute, 2011b) include two Global Information Assurance Certifications (hereafter, GIAC):

- GIAC Certified Incident Handler (hereafter GCIH).
- GIAC Certified Intrusion Analyst (hereafter GCIA).

The CEH certification is another qualification offered by the International Council of E-Commerce Consultants (EC-Council, 2011; Caldwell, 2011:10). They also offer the Licensed Penetration Tester (hereafter LPT) accreditation, with CEH being a prerequisite. The qualification requires candidates to sign a declaration of ethics (Fletcher, 2007). The Council for Registered Ethical Security Testers (hereafter CREST) is another well-known qualification in the UK (Caldwell, 2011:10). What is often unique about these training courses is that they teach the participant the same techniques used by the black hat community. The literature points out that teaching security specialists hacking techniques is essential, given that only then would they comprehensively understand the subject matter (Sanders, 2006:5). Others feel that candidates should only be allowed to attend ethical hacking training after they have undergone a thorough screening process to ensure only trustworthy individuals participate in such training (Srikanth, 2006:2). What is imperative, though, is for educational institutions to include ethical and legal lessons in their curricula. Teaching a young aspirant ethical hacker ethics seem to be an important consideration, thereby ensuring that the ethical hacker remains on the right side of the law (Ecclestone, 2001:20).

From an ethical perspective, ethical hackers who have obtained professional qualifications, such as CISSP, have to abide by the professional bodies’ code of ethics. If they are caught conducting illegal activity, they could lose their certification (Schultz, 2002:383-384).

There is also a growing tendency for universities to offer either undergraduate or postgraduate courses in ethical hacking. This is due to the high demand for IT security
specialists, in particular in the UK (Shifrin, 2006).

**Thematological research questions**

Based on the literature review above, the following thematological research questions can be defined:

**Ethical Hacking**
- Whether the banking sector employs only qualified ethical hackers.
- Whether the banking sector encourages its ethical hackers to complete ethical hacker qualifications.
- The extent to which ethical hackers have formal education in the banking sector.
- Whether it is understood in the banking sector that ethical hackers have similar knowledge to hackers and use hacking tools during their assignments.

**Hacking response**
- Whether ethical hackers are obliged to comply with the code of ethics of professional associations, such as CISSP.

Ethical hacking is conducted to address a particular need, in principle to address the threat of hacking. This need is explored further in the section that follows.

### 6.8 MOTIVATING THE NEED FOR ETHICAL HACKING

Hackers exploit known security weaknesses and failing security practices. Even when companies implement multiple layers of network security to protect their organisation, they can never assume their network is impenetrable. Organisations might deploy technical solutions as a deterrent against hacker attacks. The reality, however, is that firewalls and IDSs are often not enough. Often hackers attack online web-applications, which are not always protected by firewalls and IDSs (CICA, 2003:6). Expensive security measures, for example firewalls, might create a false sense of security. It is only when network security is approached from a hacker perspective that organisations realise how vulnerable their systems really are (Wack, *et al.* 2003:ES-1; Beaver, 2004:11). A successful hacking attempt could be expensive to remedy, could be resource intensive and might also lead to reputational losses. The loss of millions of customer records could lead to huge reputational losses and a considerable inconvenience for the customer and the organisation (SmartReply, 2007). Only when testing the network defences from the outside will the organisation obtain a detailed picture of the status of its network security (Brandt & Vines, 2001; Krutz & Vines, 2001:472). Only penetration testing can mimic the potential losses an organisation could suffer due to a hacker breach (Trull, 2012:21).
Wireless technologies and mobile computing devices are pushing the network boundaries beyond the physical walls of an organisation. This poses a challenge for organisations in adequately securing their network and systems. It also broadens the possible access points for hackers, increasing the likelihood of a successful hacking attempt (Pelkari & Fogie, 2002:77; Friedman & Hoffman, 2008:160-161). Poor security configuration is one of the common causes of security vulnerabilities (McAdam, 2007:3). Moreover, the need for ethical hacking is driven by the necessity to improve the network security posture of the organisation. It is also important to refer back to discussions in chapter 3, where the highly motivated nature of hackers was presented. It was documented in section 3.8 that there are numerous weaknesses present in organisations, which are exploited by hackers. They range from physical, logical access control, software, hardware and global interconnectedness weaknesses. The human factor has also been highlighted, which illustrates that hackers target not only technical vulnerabilities. The likelihood that at least one or more of these weaknesses exists within an organisation is very high. This further emphasises the need for ethical hacking, which can identify all of these weaknesses.

Furthermore, in section 3.10 it was documented that hacking is closely related to cybercrime in general. Reference was made to various examples of financial losses. Cybercrime security surveys highlighted the significance and extent of cybercrime attacks. Hackers engage in cybercrime for financial gains, which increase their determination and the likelihood of attacks. Examples of hacking incidents reported in the media and in South Africa in particular were highlighted in sections 3.12.2 and 3.12.3. The surveys referenced in 3.12.5 further emphasised the significance of hacking within the business context. This lends additional support to the need for ethical hacking.

Now that the need for ethical hacking has been identified, the application of ethical hacking will be discussed next.

### Thematological research questions

Based on the literature review above, the following thematological research questions can be defined:

**Ethical Hacking**
- Whether the banking sector realises that reputational risk can be averted by engaging in ethical hacking.

**Hacking response**
- Whether the need for ethical hacking is recognised in the banking sector, due to the inherent limitations associated with traditional security technologies.
6.9 THE APPLICATION OF THE ETHICAL HACKING RESPONSE

The definition of ethical hacking discussed earlier in section 6.2.3 highlighted that ethical hacking encapsulates the process of using hacking techniques to find vulnerabilities in an organisation’s defences. It has also been pointed out that ethical hacking has a multi-faceted nature. Summary Table 5.5 makes it clear that not all responses to hacking are equally comprehensive. It is therefore necessary to explore the application of ethical hacking.

The application of ethical hacking is explored from four viewpoints that have been identified following an extensive literature review. The first being as a means of improving an organisation’s network security posture. The second points out that ethical hacking improves application security during software development. The third argues that ethical hacking enhances the risk management process, in particular when identifying IT risks. The fourth argues that ethical hacking is a tool to augment the effectiveness of other hacking responses.

6.9.1 Improving information security through ethical hacking

Increasingly, organisations are using ethical hacking to test the effectiveness of their information security. It removes the guesswork associated with other remedial type approaches, such as rudimentary checklist reviews (CICA, 2003:2, 3), which may be encountered when using security configuration benchmarks, as discussed in section 5.9.3. Tiller (2005:8-9) argues that ethical hacking can be approached from two viewpoints:

- **A complete approach to information security.**
  In this approach, ethical hacking is seen as the main driving force behind securing an IT environment. It relies on the principle of discovering every possible vulnerability in the organisation’s system. The more rigorous the testing, the more secure the system.

- **Part of a larger information security strategy.**
  The security strategy includes a comprehensive assessment of the security risk. Penetration testing could be used as a form of measurement in this risk assessment. The overall results will drive the security policy and programme.

These two approaches are discussed in the sections that follow.
6.9.1.1  **Ethical hacking as a complete approach to information security**

Ethical hacking is increasingly regarded as one of the best ways of testing and improving an organisation’s network security posture (Ke, et al. 2009:460). Ethical hacking allows the organisation to assess the adequacy of its information security defences (MIS Corporate Defence Solutions Ltd., 2000:6). Ethical hacking assignments have become paramount in testing the adequacy of an organisation’s security practices and also ensuring that sensitive corporate data is safeguarded (CICA, 2003:2, 3; Fried, 2006:409; SmartReply, 2007). This is in particular where ethical hacking plays a role, in that ethical hacking is a more accurate and up-to-date means of testing the organisation’s information security posture. It will consequently address the risks that also threaten the business objectives of an organisation.

Weissman (1994:270) sees penetration testing (or ethical hacking) as a holistic security assurance process, finding flaws in the following areas: policies, specifications, architecture, software, hardware, human interfaces, configuration controls and documentation. Effectively, ethical hacking assignments can be scoped to include a review of not only technical security controls, but also general controls.

It is submitted, however, that this approach might only be practical for organisations with a medium to low dependency on IT. For organisations with a high dependency on IT, ethical hacking as part of a larger information security strategy might be more appropriate. This is discussed next.

6.9.1.2  **Ethical hacking as part of a larger information security strategy**

Arguments are made in the literature that ethical hackers assess the strengths and weaknesses in an organisation’s defences and consequently they become essential in the organisation’s information security process (Gregg, 2006:31; Caldwell, 2011:10). In order to understand fully the likelihood and impact of successful hacking attempts on an organisation, it is imperative to perform a threats assessment on the organisation itself (Pipkin, 1997:4). Ethical hacking could be a key contributor towards identifying information security risks and threats, while providing an independent opinion of an organisation’s information security.

Gregg and Kim (2005:7) argue that ethical hacking assignments can be conducted in three levels of assessments, to augment other information security initiatives:

- **Level 1 – Policy assessments:** A review of the organisation’s policies, procedures and guidelines is conducted to determine whether they adequately address all potential
risks.

- **Level 2 – Network evaluations:** This includes level 1 assessments, plus gathering information and conducting vulnerability assessments of the network environment.

- **Level 3 – Penetration tests:** This includes some elements of levels 1 and 2, but focuses more specifically on conducting actual penetration testing.

An organisation might invest substantial amounts of capital in upgrading its perimeter security, or alternatively it can take the approach of testing its security to uncover the IT vulnerabilities (Brancik, 2005:67; Schleifer, 2006). Identifying all known vulnerabilities is essential, since a hacker would pursue the weakest entry point, as opposed to attacking a well-secured target (Oppleman, *et al.* 2005:250). Ethical hacking can be an inexpensive means of testing network security when using open source hacking tools. It delivers tangible results through accurate identification of the security weaknesses (Tiller, 2005:10). Ethical hacking should be a routine part of testing the organisation network and IT system security (Wack, *et al.* 2003:ES-1) and information security practices. On-going ethical hacking assessments are essential in combating hacking risks (Oppleman, *et al.* 2005:249).

An important consideration here is that the test should be conducted by a reputable ethical hacker or red team, to provide the required level of confidence. Ethical hacking exposes significant security weaknesses in an organisation and also recommends solutions, which will address the security weaknesses. It provides a more accurate assessment of the organisation’s network security defences (Hartley, 2006:3) and remedial action can be incorporate into information security initiatives. An ethical hacking assignment might provide some conclusive evidence to persuade non-IT-literate senior managers and directors of the potential impact of a hacker attack. This may increase their willingness to provide more funding, time or resources to correct the security deficiencies (Fried, 2006:211; Hartley, 2006:3).

Some information security consultants conduct ethical hacking as part of a bigger information security assessment. Some companies might opt for automated penetration testing tools, such as Core Security Technologies. However, there is a disadvantage associated with such an approach, in that it might look for standard vulnerabilities only. A professional ethical hacker might be able to identify new and unique security vulnerabilities, when conducting the assignment manually as opposed to via automated tools (McElligott, 2006:41-42).

Like Gregg and Kim, the writers Osborne and Bavisi are both of the opinion that an
organisation may decide to use ethical hacking as a means of measuring compliance with the organisation’s security policies, which may form part of the organisation’s information security initiatives. This could include scanning emails and sniffing network traffic. Employees of the organisation have to be made aware of this in order to ensure that there is no legal infringement of their privacy (Osborne, 2006:77-78; Bavisi, 2010:258). Nonetheless, ethical hacking could contribute towards the overall improvement of IT policies and procedures (Wack, et al. 2003:ES-1; CREST, 2008).

The board of directors, audit committee, customers and other stakeholders require assurance that business information and systems are protected from malicious attacks. Legislation such as the Gramm-Leach-Billey Act and the SOX in the US require organisations to ensure that their information achieves the information security objectives of privacy, confidentiality and integrity. Ethical hacking is a means of providing this assurance to all the required stakeholders (CICA, 2003:2). A further incentive could be that ethical hacking decreases the investment in security technologies, since it is argued that ethical hacking enables information gathering of highest areas of information security risk, towards optimum investment decisions (Böhme & Félegyházi, 2010:21).

It is critical though that, when conducting ethical hacking and consequently discovering vulnerabilities, management takes remedial action. Ethical hacking will serve no value when numerous vulnerabilities are reported, without immediate remediation. Ethical hacking then becomes part of a bigger picture: the organisation’s information security governance (Schneier, 2007). As such, a number of frameworks incorporate the use of ethical hacking as a foundation for improving information security. These are discussed next.

6.9.1.3 Frameworks that use ethical hacking for improving information security

One particular framework, which stands out above the rest, is the Open Source Security Testing Methodology Manual (hereafter OSSTMM), which strongly supports the use of penetration testing (Halfond, 2010:124). OSSTMM is a comprehensive guide for Internet security testing. It aims at ensuring that thorough ethical hacking assignments are conducted and serves as a benchmark for ethical hacking assignments (Khare, 2006:195; Bavisi, 2010:258; Aylward, 2011). It can also be used as a general information security framework.

The best practice framework for information security, ISO 27002, refers to penetration testing only once, as part of technical compliance testing (ISO/IEC 2005:105), although ethical hacking could be used more extensively as a tool in many of the other sections.
Also, a standard followed in the UK for government networks and infrastructure, the CESG IT Health Check scheme (known as CHECK), was aimed at identifying known vulnerabilities in IT systems and networks which may impact the confidentiality, integrity and availability of information (Khare, 2006:194-195; Vernersson, 2010:15). This standard has now been replaced by a non-profit organisation in the UK, entitled CREST, which accredits ethical hacking specialists deployed in the industry (CREST, 2008; Leonhardt, 2010:99). An organisation that provides similar accreditation is Tigerscheme, which offer various training courses (through universities) and membership (Leonhardt, 2010:99; Tigerscheme, 2011).

Next, the work done by CERT on managing the insider threat should also be considered. CERT has been collecting empirical data on insider incidents since 2001. It has developed the Management and Education of the Risk of Insider Threat (hereafter MERIT) Insider Threat Risk Mitigation Framework, which will "empower organizations to develop comprehensive, efficient, and justifiable defenses against insider threats along with the organizational understanding and support needed to maintain a strong security posture over time" (Cappelli, Moore & Trzeciak, 2009:10, 11). Its work has developed 16 best practices that could assist an organisation in the prevention or early detection of insider incidents (Cappelli, Moore, Trzeciak & Shimeall, 2009:27).

Over and above the frameworks mentioned above, there are also custom designed methodologies that are unique in their application and may focus on a particular technology, such as Web application security. As an example, Scambray and Shema (2002:20) defined their own methodology which could be used for Web hacking and consists of various steps followed in the assessment of the web-application, including profiling the infrastructure and attacking the management interface. Furthermore, there are various general guidelines, which include aspects of vulnerability assessments, or ethical hacking that point to this last, but in the context of this thesis, important response to hacking:

- IT Audit Checklist: Information Security (IT Compliance Institute, 2006).
- Penetration Testing Execution Standard (hereafter PTES) (The Penetration Testing
Complementary to the security technologies discussed in section 5.9.4 and the methodologies discussed in this section, brief reference will be made to vulnerability databases. These are global databases, which log and categorise mostly software vulnerabilities disclosed by the public and vendors. As discussed in section 3.3.6, white hat hackers (and ethical hackers) could contribute by discovering and disclosing software vulnerabilities. Examples of these databases include the Open Source Vulnerability Database (hereafter OSVDB, 2010), Common Vulnerabilities and Exposures (hereafter CVE) (The MITRE Corporation, 2010a), the National Vulnerability Database (hereafter NVD) (NIST, 2010a) and the Security Content Automation Protocol (hereafter SCAP), which is aimed at IT security compliance automation (NIST, 2010b). Vulnerability assessment and exploitation tools make use of these databases’ classifications (The MITRE Corporation, 2010b). Ethical hackers will also consult these databases during ethical hacking assignments.

6.9.2 Using ethical hacking to enhance application security during software development

From a software development perspective, Smith, et al. argue that ethical hacking should be used during system development, as part of a larger security programme, towards increasing the security of the organisation as a whole (Smith, et al. 2002:377). It has been pointed out in section 3.9.3 that organisation are increasingly making use of web applications. Internet facing web applications are often a target for hackers and are not always protected by firewalls and IDSs. Web application security is therefore of importance. Penetration testing of web applications during development has become essential (Halfond, 2010:121). The same principle will apply to all applications used by an organisation.

Penetration testing is often conducted at a late stage of the SDLC to identify software vulnerabilities. Although this practice is beneficial in identifying software vulnerabilities due to project delivery time pressure and budget constraints, the ethical hacker might have limited time to complete the penetration testing assignment. Only a limited number of vulnerabilities might be discovered with this approach (Arkin, Stender & McGraw, 2005:84). Some organisations avoid penetration testing once the application is in production and perform it instead immediately after the development of the application (Geer & Harthorne, 2002:194; Xiong & Peyton, 2010:174). A more prudent approach would be to perform penetration testing as early as possible during the SDLC (during unit and system testing), and it should
be conducted repeatedly to identify as many software vulnerabilities as possible (Geer & Harthorne, 2002:194; Arkin, et al. 2005:86; Ardi, 2008:57-58). It can be further augmented through code reviews and the use of automated tools (Arkin, et al. 2005:85). Application or software penetration testing involves finding unexpected flaws in functionality, rather than testing the application for predictable results (Geer & Harthorne, 2002:189; Thompson, 2005:66).

It is imperative to design and build applications with security in mind. Essentially this involves applying an ethical hacking mindset. For example, when conducting code reviews, the developer might look for code errors that could be exploited by a hacker. Knowledge of ethical hacking augments the security of the application being developed. Penetration testing, as a supplementary approach, is conducted towards the end of the development lifecycle as a means of confirming that most significant vulnerabilities have been identified (Harper, 2010:12; Khan, 2010:15). Testing is not limited to applications only, but also needs to extend to operating systems, middleware and network perimeter security devices (Talukder, Maurya, Santhosh, Jangam, Muni, Jevitha, Saurabh, & Pais, 2009:4).

Similar to the frameworks discussed in section 6.9.1.3, there are a number of frameworks promoting the use of ethical hacking, with a particular focus on software development. This is discussed next.

6.9.2.1 Frameworks that use ethical hacking as part of software development

Predominantly three frameworks, identified from an extensive literature review, support the use of ethical hacking during software development: Open Web Application Security Project (hereafter OWASP), Software Assurance Maturity Model (hereafter SAMM) and Microsoft’s Security Development Lifecycle (hereafter MSDL).

OWASP strongly supports the use of penetration testing (Halfond, 2010:124). OWASP is an open source community project aimed at assisting web developers, vendors and security professionals alike to secure web-based applications through the development of software tools and documenting an informative knowledge base (Khare, 2006:195; Vernersson, 2010:15). This ensures that web applications are developed more robustly to guard against hacker web application attacks, such as those discussed in section 3.9.3. OWASP provides comprehensive guidance to software developers (in particular web-application developers) on how to conduct software code reviews. It takes the viewpoint that software vulnerabilities originate from the source code, which should be the starting point for vulnerability
identification. It provides guidance in the verification of data validation, authentication, session management, authorisation, cryptography, error handling, logging, secure configuration and network architecture (OWASP Foundation, 2008:4, 15; Xiong & Peyton, 2010:174).

An affiliated project with OWASP is the SAMM, which can also be used to implement the necessary processes to ensure the development of secure software (Chandra, 2009:3). SAMM defines detailed objectives for ethical hacking-related subjects, such as threat identification, vulnerability identification during code reviews, penetration testing of software releases, and vulnerability management (Chandra, 2009:46, 62, 66, 70). The third methodology to take note of is MSDL. It is the software development methodology followed by Microsoft developers, as well as external application developers for Microsoft. There is a strong focus on developing applications with security in mind. The methodology specifies that for “critical” applications, manual code reviews, penetration testing and vulnerability analysis should be carried out (Shostack, 2009; Microsoft Corporation, 2010:3, 12, 13). These frameworks and guidelines provide processes and structure for software development and ensure that applications are developed to include security from the onset.

6.9.3 Ethical hacking as a risk management strategy

Ethical hacking could be an integral part of an organisation’s risk management practices or ERM function (Wack, et al. 2003:ES-1; CREST, 2008). King II and King III require management to comprehend their IT systems and associated risks and threats. It follows that they also need to understand how ethical hacking can play a role in managing the risks associated with hacking and how ethical hacking could be used as an effective risk management tool, which complements management’s governance responsibilities (Voogt, et al. 2008:17; IoD, 2009b:87). Beaver (2004:10) argues that ethical hacking is “part of an overall information risk management program that allows for ongoing security improvement.” Beaver sees it as an approach to improving information security within the business (Beaver, 2007b). Beaver recognises that ethical hacking will be effective only when it is done on a regular basis, with a particular contribution to information risk management. He points out that ethical hacking cannot be effective if it is not integrated into the information security programme of the organisation, which includes at least the following components (Beaver, 2004:334):

- High-level risk assessments.
- Compliance with security policies.
Incident response and business continuity processes.

Security awareness and training.

It has already been indicated in section 5.4.3 that IT risk management should be used to identify the risk of hacking. It follows that an appropriate mechanism needs to be found to assist with this task. With this in mind, ethical hacking is sometimes seen as a risk management tool (Padayachi & Keyser, 2008; Voogt, et al. 2008:11, 17). Vulnerability assessments and penetration testing are at times conducted as part of risk assessments of an organisation’s information systems (Wu, 2007:40). Alternatively, ethical hacking augments risk management practices towards effective identification of system vulnerabilities (Alaboodi, 2007:34).

There are literally thousands of potential vulnerabilities that might be of a concern to an organisation. Yet organisations have limited funding available and cannot address all possible vulnerabilities. Ethical hacking is a means of assisting the organisation in effectively identifying key risks, while the risk management process will aid in ranking and prioritising the risks appropriately. The limited funding can then be used effectively to address significant vulnerabilities (Cardholm, 2006:15; Whitaker & Newman, 2006:4; Harris, 2008:81). The ethical hacker is in the best position to assess the risk and likelihood associated with a particular vulnerability. When articulating the vulnerability as a risk, the potential impact and possible monetary loss might create a better understanding among senior management and lead to earlier resolution (Chapela, 2010:7).

Penetration testing may be used as a means of quantifying the risk of hacking in order to highlight the significance of a potential hacking incident. The key is to present the hacking risk scenario as a business risk to the board of directors, senior management and operational staff, to obtain their support and buy-in (Van den Berg, 2009). Once vulnerabilities have been identified through penetration testing, the knowledge of those vulnerabilities should be shared across the organisation through the risk management and governance processes. This will ensure that the same vulnerability does not recur in another part of the organisation (in particular in large organisations), which may provide alternative avenues for hackers to exploit (Harper, 2010:12).
6.9.4 Ethical hacking augmenting the effectiveness of other responses to hacking

Ethical hacking can be expanded to assess the effectiveness of some of the responses discussed in chapter 5. As it has been indicated, the responses to hacking are not always comprehensive enough to cover all the IT risk themes identified. Moreover, depending on the maturity and comprehensiveness of the response, or the lack thereof, hackers may succeed despite the presence of the identified responses. The role of ethical hacking in improving an organisation’s information security, software development practices and risk management have already been discussed in this chapter. It is argued that ethical hacking could assist with augmenting some of the other responses identified in chapter 5, such as the corporate governance processes (including IT governance), information security controls, security technologies and baseline security configurations. Effectively, this leads to a multi-layered response to hacking, leveraging of and augmenting other governance response followed by the organisation (Roos, Voogt & Marx, 2011:21-22).

6.9.4.1 Ethical hacking augmenting the corporate governance response

It is submitted that the board of directors often does not understand the concept “ethical hacking” and how it can address the risk of hacking. With King III placing the responsibility of IT governance on the board of directors, security assessments, which may include ethical hacking, need to be considered (Van den Berg, 2009). Ethical hacking can strongly support the corporate governance response when it is linked via information security or IT governance frameworks, such as ISO 17799 or CobiT (Padayachi & Keyser, 2008; Van den Berg, 2009). Furthermore, an ethical hacking assignment on its own would not be effective if it is not integrated with the organisation’s corporate governance processes, such as the risk management processes (Gupta, 2008). Furthermore, it is submitted that ethical hacking will not be effective if the security weaknesses are not remediated by the organisation’s internal processes, such as updating the baseline security configuration and feeding the information into the patch management council, to ensure the latest patches are applied.

An ethical hacking assignment might include more than solely an attempt to break into a target system. The assignment might also include a review of the operational processes of the organisation, for example reviewing the vigilance of the helpdesk function and/or a review of the physical security, which are processes defined under IT governance. The objective still remains the same in that the ethical hacker will try to circumvent either the operational process or the physical security (Tipton & Krause, 2006:204).
Internal control is a requirement of good corporate governance. As a comprehensive approach, ethical hacking could be used to test several distinct areas of controls: network controls, application controls and physical security controls (Osborne, 2006:258), thereby providing an assessment of an organisation’s internal control. Given that hackers could easily circumvent internal control, ethical hacking can be used to assess the system of internal control to ensure it prevents hacker attacks (own deduction).

6.9.4.2 Ethical hacking augmenting the security technologies response

It has already been mentioned in section 6.8 that expensive security measures can create a false sense of security. Ethical hacking is a means of testing these security technologies, such as firewalls and encryption, to assess whether they provide the required security as promoted by the product vendors (Beaver, 2004:11). It is argued that firewalls and network security should be tested by ethical hacker service providers at least annually (Glascock & Gaulke, 2010:56). Ethical hackers consider hacking attack techniques that circumvent the controls implemented by security technologies. Therefore, the results of the ethical hacking assignment might highlight that alternative configuration options might have to be applied for security technologies, to ensure they will prevent a myriad of hacker attacks (Harris, et al. 2005:12). Vulnerability assessment and penetration testing results can assist with the correct placement of IDSs (Brancik, 2005:493). There are also numerous hacking tools available to test security technologies, such as the tool “Firewalk” for firewalls, or attack techniques for IDSs and IPSs, such as IDS and IPS evasion through network traffic manipulation (Skoudis & Liston, 2006:301, 322-323). These are effective mechanisms of testing the robustness of security technologies.

6.9.4.3 Ethical hacking augmenting the baseline security configuration response

Baseline standards and configurations are the starting point for a well-secured system (Klevinsky, et al. 2002:30). Many IT systems and network devices require secure configuration. Poorly configured IT systems and network devices are popular attack vectors for hackers. Vulnerabilities discovered during an ethical hacking assignment can often be remediated by implementing best practice configuration of systems and supporting infrastructure. This refers to the technical systems level, where configuration settings often determine the security (or otherwise) of the system in question (McAdam, 2007:3). Furthermore, once configuration errors have been identified, the ethical hacker could recommend best practice configuration settings to remediate the configuration errors (Klevinsky, et al. 2002:30). Alternatively, ethical hacking can be used to test the
effectiveness of baseline standards and configurations.

6.9.4.4 Conclusion

Ethical hacking is more than merely providing a view on whether an organisation can withstand a hacker attack. Ethical hacking can improve an organisation’s information security posture by assisting with the identification of information security risks. It provides convincing evidence of security weaknesses, software vulnerabilities or a lack of security controls, increasing the probability of senior management taking remedial action. There are also a number of frameworks that provide guidance on how ethical hacking assignments could be conducted in order to improve information security.

Ethical hacking is also effective in enhancing application security, already during development of the application. Developing applications with an ethical hacking mindset will lead to fewer software vulnerabilities and produce a more secure system in general. Again, there are a number of frameworks that could assist with improving software security, such as OWASP and SAMM.

Ethical hacking can also be applied during risk management processes, to accurately determine the likelihood and impact of hacker attacks or related IT risks. Combining ethical hacking with the organisation’s risk management strategy becomes an effective means of identifying and prioritising information security vulnerabilities.

Ethical hacking can augment a number of responses to hacking. It can augment the corporate governance response, when integrated with the information security and IT governance processes of the organisation. Ethical hacking could also be effective in identifying weaknesses in the governance processes and to test the effectiveness of internal control implemented to prevent hacker attacks. Ethical hacking can in particular augment the information security response, which could assist with establishing adherence to information security policies and procedures. Ethical hacking can also be used to test various security technologies and baseline security configurations, to ensure they provide the protection as required by the organisation.

Ethical hacking is not without risk. There are both advantages and disadvantages associated with ethical hacking, and these are explored in the following two sections.
Thematological research questions

Based on the literature review above, the following thematological research questions can be defined:

Hacking Response

- The extent to which ethical hacking is used as part of a larger security strategy in the banking sector.
- The extent to which ethical hacking is used as a complete approach to information security in the banking sector.
- The extent to which ethical hacking is integrated with the banking sector's corporate governance and IT governance processes.
- The extent to which ethical hacking is integrated with the banking sector's information security, risk management and assurance processes.
- The extent to which ethical hacking is used to test internal control in the banking sector.
- The extent to which the banking sector makes use of ethical hacking to improve its network security posture.
- The extent to which ethical hacking is used in the banking sector to provide an independent opinion of a bank's information security posture.
- Whether ethical hacking is used to provide conclusive evidence to persuade management of the threat of hacking in banking sector.
- Whether ethical hacking is used only on an ad hoc basis, or whether it is used routinely in testing the banking sector's information security.
- The extent to which ethical hacking is used in the banking sector to identify security vulnerabilities.
- Whether frameworks such as OSSTMM and MERIT are known within the banking sector.
- The extent to which the banking sector applies ethical hacking during software development.
- Whether ethical hacking is used only once off or repeatedly throughout software development.
- Whether frameworks with a focus on making use of ethical hacking during software development, such as OWASP, SAMM and MSDL, are known in the banking sector.
- Whether ethical hacking is used to prioritise security vulnerabilities or IT risks as part of the banking sector's risk management processes.
- Whether ethical hacking is used to achieve compliance with organisational policies and relevant legislation in the banking sector.
- The extent to which ethical hacking is used to test the effectiveness of security technologies and baseline security configurations in the banking sector.
- The extent to which the banking sector makes use of ethical hacking to test the internal control measures implemented to prevent and detect hacker attacks.

6.10 THE ADVANTAGES OF ETHICAL HACKING

Ethical hacking has several advantages and benefits. The benefits are perhaps best embodied in the quote by Smith, et al. (2002:377):

Penetration testing by ethical hackers is amongst the most thorough methods for finding vulnerabilities and increasing protection for a dynamic network of computers.

Ethical hacking assists an organisation in taking preventative steps against attacks from hackers, while actively remaining within the letter of the law (EC-Council, 2011). Ethical hacking will also help the target organisation to determine its ability to withstand an attack.
Furthermore, ethical hacking might highlight obvious vulnerabilities that could require the immediate rectification of identified security weaknesses. Ethical hacking may also identify new and emerging vulnerabilities, contributing to the overall improvement of information security in the public domain. Ethical hacking might identify weaknesses that may not otherwise be identified through automated scanners or checklist audits (Cohen, 1997; McCollum, 2003). Vulnerability assessments assist system administrators with the onerous task of identifying vulnerabilities and patching them accordingly (Farmer, 2006:24). Automation of security testing is emphasised in the literature as a way of achieving significant time savings in security testing (Tillman, 2010:50; Samant, 2011:15). It therefore alleviates some of the operational burden associated with ensuring system security.

In contrast, management might fail to take notice of the information security weaknesses. This might be due to a lack of technical knowledge or awareness of the likelihood of the risk. Identifying the vulnerabilities through ethical hacking and demonstrating the potentially devastating impact on systems are an effective means of obtaining management’s attention and buy-in (Cohen, 1997; McCollum, 2003; Wright, 2008:4). This will also avert possible reputational consequences.

Another advantage of ethical hacking is that it can be seen as a comprehensive approach towards assessing the likelihood of various types of hacker attacks, such as non-technical attacks, network-based attacks, operating system and application-based attacks (Beaver, 2007a:14-15) and other attacks as discussed in section 3.9. It can assist an organisation in prioritising identified security issues, ensuring efficient use of the available security budget (Samant, 2011:10). Penetration testing exposes weak security practices, which may have gone unnoticed via manual assurance or security reviews (Trull, 2012:24). Moreover, Tiller (2005:88, 90, 91) provides the following advantages associated with ethical hacking:

- Ethical hacking identifies technical vulnerabilities.
- The exposure and likelihood of a particular threat is determined by ethical hacking.
- The total amount of effort or complexity required to exploit a vulnerability is determined.
- Provides an objective independent assessment of the organisation’s IT infrastructure.
- Provides a very comprehensive assessment, when using scanning or vulnerability assessment tools.
- Provides information on the tools hackers would most likely use to attack a particular IT technology being used by the organisation.
• Assesses the likelihood of internal attacks and social engineering.
• Accurately reflects a particular threat.

As pointed out in section 6.6, conducting ethical hacking in conjunction with IT staff means that they can benefit from the experience by learning more about their network environment and understanding the possible entry points for hackers. In turn, IT staff could point out the critical systems, allowing the ethical hacker to focus his efforts on finding vulnerabilities in those critical systems (Klevinsky, et al. 2002:26).

Ultimately, it is not only information security that benefits from ethical hacking. The business itself has many benefits to derive from ethical hacking (Corsaire Limited, 2007):
• It will assist the organisation in averting substantial financial losses due to hacker breaches.
• Where compliance is required with industry standards, ethical hacking plays a role in achieving the required compliance.
• The ability to prevent hacker attacks will add to the reputation of the company.
• A more accurate risk assessment of hacking may be conducted, which will ultimately lead to cost savings in implementing appropriate solutions.

Ethical hackers minimise the reputational risk confronted by an organisation by finding significant vulnerabilities before a hacker does. This enhances system security and prevents the likelihood of further attacks. When used to test the security of online applications in particular, finding vulnerabilities could save the organisation from significant embarrassment should a hacking incident occur (Smith et al. 2002:377).

Ethical hacking can be an inexpensive means of testing the organisation’s network security. It delivers tangible results, through accurate identification of the security weaknesses (Tiller, 2005:10; Hartley, 2006:3). Because of the hands-on practical component of penetration testing and the visual effect of demonstrating how the security is compromised, penetration testing results create “a sense of urgency” when presented to management (McElligott, 2006:42; Chapela, 2010:7). Penetration testing also reduces the probability of hacking or other similar threats (Ardi, 2008:2). One of the key benefits in performing ethical hacking is that it is by far a more risk averse approach in allowing an ethical hacker to discover vulnerabilities, which is confidentially remediated inside the organisation, as opposed to a grey hat hacker discovering the vulnerabilities and publicly disclosing them (Raywood, 2011).
Furthermore, ethical hackers can provide insightful views on the interaction of various security measures and processes, in particular from a technical perspective, while identifying the gaps in the layered security defences of an organisation (Herzog, 2011).

## Thematological research questions

Based on the literature review above, the following thematological research questions can be defined:

### Hacking Response

- The extent to which the banking sector makes use of ethical hacking to identify security vulnerabilities in its organisations.
- The extent to which the banking sector uses ethical hacking to test the likelihood of various hacker attacks, such as social engineering, being successful.
- Whether the banking sector makes use of ethical hacking for industry compliance.
- The extent to which the banking sector makes use of ethical hacking as a means of risk assessing the likelihood of hacking taking place.

### Business risk

- Whether the banking sector makes use of ethical hacking to avert potential reputational losses due to hacker attacks.

## 6.11 THE RISKS AND DISADVANTAGES ASSOCIATED WITH ETHICAL HACKING

Organisations making use of ethical hacking have to familiarise themselves with the risks and disadvantages of ethical hacking, in order to proactively manage these. An extensive literature review has revealed several risks and disadvantages that have been grouped together, and these are discussed in the sections that follow.

### 6.11.1 Risks and disadvantages associated with simulated hacking activity during ethical hacking assignments

There is often a negative association with the concept “ethical hacking”. The act of hacking itself is regarded as unethical (Graves, 2007:7; Caldwell, 2011:11). The term “hacking” carries with it a negative connotation (EC-Council, 2008a:32). Since the concept “ethical hacking” contains the word “hacking”, automatically it is assumed to have a sinister or malicious connotation (Gupta, 2011a).

Ethical hackers may be tempted to use their skills to demonstrate to an organisation that they can break into their network. This may be done to attain a business opportunity. This
kind of behaviour is regarded as “immoral, unethical and unprofessional” (Cohen, 2002). This type of behaviour would instead be associated with white hat hackers, who sometimes test the boundaries of what is considered ethical.

Since ethical hacking mimics what hackers do, the ethical hacker might find himself walking a very thin line between adhering to and breaking the law (Pipkin, 1997:7). In particular, when conducting ethical hacking with no restrictions, the likelihood that a client’s system may be affected increases, which might have legal implications (Knight, 2009:39). From a South African perspective, section 86 of the ECT Act (RSA, 2002:55) deals with the unauthorised access to, interception of or interference with data (Herselman & Warren, 2004:256). The key for the ethical hacker is to obtain explicit authorisation before commencing with ethical hacking activity. If not, an ethical hacker could be found guilty of an offence. The same applies to the distribution of devices and software that are primarily used to circumvent IT security measures, which is regarded as a criminal offence (Magele, 2005:10). Ethical hackers have to make sure that they do not share ethical hacker tools with criminals who might use them for personal gain.

A number of risks that could materialise during an ethical hacking assignment, which could cause significant damage to the organisation:

- During a penetration test, confidential information might surface. The ethical hacker might be tempted to steal the information for financial gain (Cohen, 1997).
- The penetration tests conducted may affect the system in such a way that new system vulnerabilities are introduced (Cohen, 1997).
- The ethical hacker might have obtained access to business critical applications, which could be misused (Matusitz, 2006:282-283).
- System administrators might be startled when seeing traces of the attack. The network performance might be affected or systems might even crash as a result of some ethical hacking activities (Palmer, 2001a:776; Sholomyansky, 2007:4, 9, 13; Bavisi, 2010:263).
- There is also the possibility of an ethical hacker changing system or router settings as proof of system compromise. However, management will take a dim view on adverse influences on their production environment (Klevinsky, et al. 2002:27). It is therefore essential for the ethical hacker to agree the extent of his testing with management prior to the assessment.
- Critical or sensitive infrastructure, such as power utilities or gas refineries, might be affected by penetration testing. These should rather be tested in a test environment.
6.11.2 Risks and disadvantages associated with ethical hacking assignments and the outcome thereof

Penetration testing, at times, might not be a comprehensive or methodical approach to identifying vulnerabilities. The ethical hacker might only provide proof that it is possible to hack into a system, rather than identifying all possible vulnerabilities. Vulnerability assessments (in particular those conducted by making use of automated tools) might provide a long list of vulnerabilities, without specifying how they can be exploited. The actual interpretation and remediation of those vulnerabilities might be challenging (Poolsappasit, 2010:3, 27; Leonhardt, 2010:96).

Tiller (2005:88, 90) provides the following disadvantages associated with ethical hacking assignments and their outcome:

- Ethical hacking does not consider the management practices and security policies being used (when focusing on penetration testing).
- Ethical hacking observations are very specific and do not provide recommendations regarding aspects around the observation.
- Ethical hacking does not consider asset value (sensitive and critical business systems might be more secure and vulnerabilities might be discovered on less critical systems).
- The success of an ethical hacking assignment is dependent on the skills and competencies of the ethical hacker.

Moreover, Gupta warns that ethical hacking does not provide complete assurance that the organisation is impenetrable or without security weaknesses. He is of the opinion that ethical hacking and a combination of information security and user awareness will reduce weaknesses. He makes a vital statement regarding organisations that are “stagnant” in assessing their information security. These organisations will not be able to align their business strategy with the security objectives (Gupta, 2008). Ethical hacking could also be used in a scare tactic against management, who might react to fix the immediate problem, rather than address the lack of IT process and governance which led to the existence of vulnerabilities in the first place (Aylward, 2011).

Another disadvantage of ethical hacking is the need to keep up to date with the latest developments in information security and also the latest threats and vulnerabilities (Gilmore,
This could also result in a false sense of security, when an ethical hacker bases his assessment on outdated information and tools (Beaver, 2007a:13, 18). This therefore implies that the ethical hacker has to engage in ongoing training and research into the latest hacking techniques. The success of penetration testing might also depend on the knowledge and experience of the ethical hacker. The outcome of a penetration testing assignment completed by two independent ethical hackers might be completely different. Penetration testing therefore may not produce repeatable results (Engle, 2010:22; Fovino, Guidi, Masera & Stefanini, 2011:525). The same sentiment is shared by Harper, who also points out that penetration testing might only identify a limited number of vulnerabilities or information security control weaknesses. In addition, a vulnerability assessment does not provide guarantees that the network is secure (McCollum, 2003). When vulnerability assessment tools are used to identify vulnerabilities, the reports produced by these tools might be ambiguous or might contain limited information, forcing the developers or system administrators to find the solution themselves (Harper, 2010:11).

It is argued that ethical hacking could produce fewer results than a standard audit or security review (Osborne, 2006:279). Organisations might sometimes be under the wrong impression that ethical hacking will identify every conceivable vulnerability. Ethical hacking is typically done in a small timeframe and might focus on identifying the most obvious vulnerabilities. A hacker, on the other hand, could plan an attack over an extended period and might be selective in his approach, to ensure the biggest likelihood of success (Wright, 2005).

6.11.3 Disadvantages associated with the use of ethical hacking tools

Another risk associated with ethical hacking is the use of open source hacker tools. Some of these tools might be professionally developed; however, caution must be taken when using software written by hackers, since they may contain Trojans. It is advisable to scan them with anti-virus software and deploy them in a test environment, where the actions of the tool could be monitored and tested (Parker, 2006: 1.44; Khare, 2006:196-197).

Comprehensive vulnerability assessment scanning could be very resource-intensive, in particular where vulnerability assessment tools are rolled out across the organisation to identify vulnerabilities in the organisation’s systems. The tools or scanning agents should be placed strategically, to ensure that they do not disrupt normal business operations (Huber, 2003:5). Moreover, some vulnerability assessment tools feature powerful functions, which could have a negative effect on the organisation’s systems. For example, some tools will be able to test for DoS attacks. This might imply that the tools will launch a small DoS attack.
against selected targets. Should it so happen that the target systems are susceptible to this kind of attack, they may fail completely, leading to a possible business continuity scenario (Huber, 2003:6).

Using open source vulnerability assessment scanners, for example Nessus, could pose a risk under certain conditions (Tenable Network Security, 2007:5):

- Some legacy operating systems cannot cope with scans against multiple open sockets (software services provided by the operating system). The operating system might freeze during such conditions.
- Valid users can be denied access to legitimate services, when the scanner causes those services to lock out due to multiple failed login attempts.
- Due to the traffic volumes created by the scan and in combination with existing traffic, the scans could cause a DoS or general degradation of the network traffic.

Germany has updated its legislation to make it an offence to create, use or distribute hacking tools. This complicates matters for ethical hackers in that country, since their activity could be deemed illegal, even when it takes the form of justifiable information security assessments (Leyden, 2007). The UK almost made similar changes to its legislation; however, after protests from the security industry, amendments were made to the legislation to ensure criminal intent can be established (Leyden, 2008).

6.11.4 Concerns associated with ethical hacking training

The teaching of ethical hacking as part of an information security curriculum at colleges and universities is also considered a controversial practice (Simmons, 2008:1; BBC Tyne, 2008). Livermore (2007:111) indicates that with the growing threat of cybercrime, the demand for professionally trained security specialists is increasing, hence more colleges and universities are teaching ethical hacking. Livermore argues that the controversy revolves around the teaching of ethical hacking skills to young “immature” students, who might use the tools irresponsibly. Possible solutions followed by universities and colleges in addressing the risks associated with teaching ethical hacking could include completing a course in ethics; prescreening of students before admission; asking them to sign a code of conduct, and isolating the security labs from the rest of the campus network (Livermore, 2007:113-114).

One of the possible sources where ethical hackers can obtain information on how to conduct hacking is books on hacking and ethical hacking. Harris et al. (2005:11) argue that some
critics claim that hacking books may increase the skills level of hackers. Others are in favour of hacking books, stating that they are mostly meant for security and network professionals.

6.11.5 Conclusion

As with hacking activity, ethical hacking could lead to business disruption or disclosure of sensitive business data, when not conducted with consent or by an inexperienced ethical hacker. Ethical hacking might highlight numerous vulnerabilities, without a clear explanation of how they can be exploited. Ethical hackers also need to keep themselves up to date with the latest vulnerabilities and hacking techniques. The use of open source hacking tools could also lead to business disruption, if not tested or carefully deployed. Ethical hacking training is also at times considered a controversial practice.

<table>
<thead>
<tr>
<th>Thematological research questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Based on the literature review above, the following thematological research questions can be defined:</td>
</tr>
<tr>
<td><strong>Business Risk</strong></td>
</tr>
<tr>
<td>• Whether the banking sector is receptive to the risks forthcoming from ethical hacking.</td>
</tr>
<tr>
<td>• The extent to which the banking sector manages the possible negative effects of ethical hacking assignments.</td>
</tr>
<tr>
<td>• Whether the banking sector has experienced downtime, loss of data or damage to IT systems due to ethical hacking assignments.</td>
</tr>
<tr>
<td><strong>IT risk</strong></td>
</tr>
<tr>
<td>• Whether the banking sector tests open source hacking tools before deploying them on the network.</td>
</tr>
<tr>
<td>• The measures taken by the banking sector to protect themselves against the threats inherently associated with hacker tools.</td>
</tr>
<tr>
<td><strong>Hacking Response</strong></td>
</tr>
<tr>
<td>• The extent to which the banking sector relies on the results of an ethical hacking assignment to remediate information security vulnerabilities.</td>
</tr>
<tr>
<td><strong>Ethical Hacking</strong></td>
</tr>
<tr>
<td>• The extent to which there is fear and mistrust in the use of ethical hacking in the banking sector.</td>
</tr>
<tr>
<td>• The extent to which open source ethical hacking tools are used in the banking sector and by whom.</td>
</tr>
</tbody>
</table>

6.12 DIMENSIONS OF THE ETHICAL HACKING RESPONSE

It has been established in this thesis that hacking is both a risk and an event, which can take place now and in the future. Ideally, a hacking event needs to be prevented from taking place. Figure 3.3 indicated that ethical hacking is a preventative control. Ethical hacking
aims to identify software vulnerabilities, security configuration weaknesses, and weaknesses in logical and physical access controls before they are exploited by hackers. Ethical hacking is therefore intrinsically preventative in nature.

Ethical hackers could however recommend both preventative and detective controls (Veerasamy, 2009:420). It is also possible that ethical hackers could detect signs of hacker activity (such as the purging of log files), during an ethical hacking assignment. Therefore, indirectly, it is also detective in nature.

### 6.13 ROLE-PLAYERS IN THE ETHICAL HACKING RESPONSE

Ethical hacking requires authorisation from someone senior in the organisation (pointed out in section 6.4.3). It should be a decision-maker who has the authority to allow an ethical hacking assignment, which could potentially affect an organisation’s systems. It is therefore not unlikely that the authorisation might have to be sought from the CIO, CFO or even the CEO, or at least the business owner of the system in question. These are potentially very senior role-players involved in ethical hacking. Ethical hacking could also be used as part of risk management and information security processes (highlighted in section 6.9.3). As clearly stated in King III, the board of directors is responsible for risk management, assisted by the risk committee and/or audit committee (discussed in sections 5.4.1 and 5.4.5). Directors also need to enquire as to whether security technologies are assessed via ethical hacking, as a means of determining whether the organisation protects itself from hacker attacks (Glascock & Gaulke, 2010:56). Any of these role-players might request assistance from the ethical hackers to provide a view on the organisation’s information security posture and therefore analyse the results. Other indirect stakeholders could be operational or IT staff, assisting with remediation of issues identified during ethical hacking assignments.

### 6.14 ETHICAL HACKING AS A RESPONSE TO BUSINESS RISKS AND IT RISKS

It has been highlighted in this chapter that ethical hackers use the same techniques that hackers do, although only with legal intent. It has also been argued that ethical hacking augments corporate governance and other responses to hacking. It follows that the links established between the various business risks, IT risk themes and hacking in chapter 4 would also be applicable to ethical hacking, from the perspective that ethical hacking can then be seen as a response to the threat of hacking. To demonstrate the link, each business risk and related IT risk themes will be discussed briefly:
• A hacker will use social engineering to gain unauthorised physical access, thereby compromising physical risk, as discussed in section 4.5. Similarly, an ethical hacker can test the physical access controls by means of social engineering techniques, dumpster diving and wardriving, as mentioned in sections 6.2.3, 6.4.3, 6.4.4, 6.4.6 and 6.5.2. The likelihood of theft or damage to IT equipment can also be tested by the ethical hacker during social engineering assignments.

• Employees often fail to comply with the organisation’s IT policies and procedures, compromising operational risk in the process. As discussed in section 4.6, employees might follow weak password practices and let their passwords or sensitive system details lie around on their desks. Similar to a hacker, an ethical hacker can use social engineering to find passwords or confidential system details by browsing the office area, in order to test whether unauthorised logical access would be possible, as discussed in section 6.4.6. Furthermore, operational risk may be compromised by inadequate project management practices, as highlighted in section 4.6. In section 6.9.2, the important role of ethical hacking during the SDLC of an organisation has been outlined, to ensure that software is developed to avoid application and data control weaknesses. The IT risks, inadequate IT operations and support and inefficient use of IT resources, could lead to poor systems support, leaving the organisation’s systems vulnerable to hacker attacks (as discussed in 4.4.1 and 4.6). This inevitably increases operational risk. During an ethical hacking assignment, the ethical hacker might find that the systems produce inadequate IT performance, due to a lack of IT skills or poor configuration. Ethical hackers can comment on the efficiency of organisational processes, which will clearly be evident when they have the opportunity to interact with work performed by the IT staff. When assessing an organisation’s information security practices, ethical hackers could point out systems, which have been poorly supported.

• Human behaviour plays a role in affecting human resource risk, as discussed in section 4.7. Insiders might misuse IT, committing irregularities and fraud by means of hacking techniques. Ethical hackers can test the likelihood of insider attacks, as pointed out in sections 6.4.3, 6.9.1.3. Since an ethical hacker provides an opinion on the organisation’s information security practices (as discussed in 6.9.1.2), it may include a view on the competency and knowledge of IT support staff. The ethical hacker might point out that staff do not have the necessary IT security training and by implication will assist with mitigating the risk IT human resource deficiencies. When
collaborating with insiders, hackers could escalate their system privileges, due to a *lack of segregation of duties* (discussed in section 4.4.1). Ethical hackers could carry out similar tests through social engineering assignments, as discussed in section 6.4.6.

- It was established in section 4.3.5.4 that IT risk is a sub-component of technology risk. Since hacking strongly relates to the IT risk themes identified in section 4.3.5.17 and technology risk by association (as highlighted in section 4.8), it follows that ethical hacking could also be used as a response to technology risk. Indeed, ethical hacking demystifies some of the complexity associated with technology, including the *complexity of IT* in providing a deeper understanding of in particular IT hardware and software, as highlighted in section 6.10. Furthermore, ethical hacking can be used to assess technical security technologies and baseline security configuration (discussed in sections 6.9.4.2 and 6.9.4.3). Security vulnerabilities are often found in operating systems, causing *operating system weaknesses*, as discussed in section 4.4.1. Experienced or well-trained ethical hackers might have above average knowledge of operating systems (section 6.7) and might be able to find associated vulnerabilities. *Interface/network control weaknesses* can be exploited by hackers, as discussed in section 4.4.1. Similar to hackers, ethical hackers can use sniffers (discussed in section 3.9.1.1) to test interface controls. Hackers often delete signs of their hacker activity. The *lack of audit trails* (discussed in section 4.4.1), would complicate investigations. Ethical hackers can also determine the likelihood of deleting log files and audit trails during the maintenance phase, as discussed in section 6.4.9. Regular ethical hacking assessments will not only decrease the likelihood of hacking incidents, but will also assist with the mitigation of technology and IT risks.

- One of the most debilitating attacks by hackers is DoS, which could lead to *business and IT disruption*, increasing an organisation’s business continuity and disaster recovery risk, as pointed out in section 4.9. In principle, ethical hackers can simulate a similar kind of attack. However, they typically avoid this, as discussed in section 6.2.4 and 6.11.1. As a disadvantage of ethical hacking activity and tools used, as pointed out in 6.11.2, the risk of interrupting business processing and causing a business continuity scenario cannot be ruled out, but can be managed carefully to avoid it at all costs.

- The credit and market risk of an organisation can be affected by hackers who gain *unauthorised logical access* to the organisation’s credit and market systems and post
unauthorised transactions due to application control weaknesses, as discussed in section 4.10. Ethical hackers could determine the likelihood of gaining access to business systems, although explicit authorisation will have to be obtained before posting transactions, as discussed in section 6.11.1.

- There is complexity associated with cybercrime (which includes hacking), both in prosecuting cybercriminals (and hackers) and complying with legislation to minimise or prevent cybercrime and hacking activity. This increases an organisation’s compliance risk, as discussed in section 4.11. An ethical hacker can assist by risk assessing the likelihood of cybercrime activity. Furthermore, the ethical hacker should have a good understanding of the relevant pieces of legislation (discussed in section 6.11.3) and advise management on how to avoid legal pitfalls. The use of hacking tools by ethical hackers could also increase compliance risk, as discussed in section 6.9.1.2. An organisation will have to ensure that local legislation does not restrict the use of ethical hacking tools.

- A hacker event could lead to public embarrassment and increase an organisation’s reputational risk, as pointed out in section 4.12. An ethical hacker can assist an organisation to avoid reputational consequences, as discussed in section 6.8, by identifying vulnerabilities and allowing the organisation to remediate before allowing hacker attacks to lead to public humiliation.

It is clear then that ethical hacking addresses not only each business risk, but also each IT risk theme identified in this thesis. It therefore provides a comprehensive response to the business risks and IT risk themes. Now the link with the control objectives will be explored.

### 6.15 ETHICAL HACKING AND THE LINK WITH CONTROL OBJECTIVES

Penetration testing identifies vulnerabilities in applications, which may compromise authentication, authorisation, confidentiality, integrity or non-repudiation, often with a specific focus on authentication (Geer & Harthorne, 2002:193, 194). As part of security testing, ethical hacking, penetration testing and vulnerability assessment cover the objectives confidentiality, integrity, authentication, availability and authorisation (Khan, 2010:15). Also, when ethical hacking augments information security, ethical hacking assists with the achievement of the information security objectives confidentiality, integrity and availability. Ethical hacking can be used to comprehensively test logical access controls (discussed in
section 6.4.3 and 6.14), therefore focusing on authentication and authorisation. When used to test an organisation’s technical security defences (section 6.9.1.2), the control objective security is also assessed. In section 4.4.2 and Table 4.29 the link between hacking and control objectives was explored. The discussion of each control objective and how it can be impacted by hackers applies equally to ethical hackers.

<table>
<thead>
<tr>
<th>Thematological research questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Based on the literature review above, the following thematological research questions can be defined:</td>
</tr>
</tbody>
</table>

**Hacking response**
- The extent to which there is a realisation in the banking sector that ethical hacking is a comprehensive response to business and IT risks, and in particular the threat of hacking.
- Whether ethical hacking is used in the banking sector to mitigate any of the business risks, IT risk themes and control objectives identified in this thesis.

### 6.16 CHAPTER SUMMARY

Ethical hacking is the discipline of using the same tools and techniques that hackers use, but with the intent to defend and protect an organisation against hacker attacks. This chapter has explored the definitions of ethical hacking and ethical hacker profiles. A generic ethical hacking methodology has been defined. It has been established that the concepts vulnerability assessment and penetration testing are different categories of ethical hacking, where the former focuses on identifying vulnerabilities only and the latter exploits the vulnerabilities found.

The need for ethical hacking has been identified from the perspective that organisations continue to be vulnerable to hacker and cybercrime attacks. It has been established that ethical hacking has several objectives. Ethical hacking can be used as a risk management tool as part of the information security management strategy. In particular, ethical hacking is effective in finding security vulnerabilities. It is also an essential technique to be used during software development to mitigate security control deficiencies before deploying the application. With reference to the other responses identified in chapter 5, it has been argued that ethical hacking can augment corporate governance and IT governance responses, effectively creating a multi-layered response to the threat of hacking.

The responses discussed in chapter 5 do not necessarily test IT security at a granular level. Ethical hacking has the ability to provide convincing evidence of information security
deficiencies, testing the organisation’s information security at a granular level. Ethical hacking is therefore not a stand-alone discipline with only limited application.

All the IT risk themes identified in this thesis can be addressed by ethical hacking. When ethical hacking is compared to some of the most comprehensive responses identified in chapter 5, it is evident that ethical hacking can provide a more comprehensive response. Furthermore, when it is used to augment other responses, as discussed in section 6.9.4, it further supports the multi-layered response, filling the gaps of other responses. If the comprehensive responses to IT risk themes summarised in Table 5.5 (now repeated in Table 6.5) are taken into consideration, comprehensive coverage of ethical hacking can be compared with the other responses.

<table>
<thead>
<tr>
<th>General controls</th>
<th>Ethical Hacking</th>
<th>Internal control</th>
<th>CobIT 5</th>
<th>Security Technologies</th>
<th>ISO 27002</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorised physical access / lack of physical access control and security.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lack of compliance with IT policies and procedures, legal and regulatory requirements.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business and IT disruption.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inadequate IT operations and support.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Theft or damage to IT equipment.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inadequate change / project management practices.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Misuse of IT / irregularities and fraud.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cybercrime</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unauthorised logical access.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inadequate IT performance.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Complexity of IT.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inefficient use of IT resources.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT human resource deficiencies.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Ethical hacking also supports the mitigation of both business risks and associated IT risks themes. Using Table 4.32 as a base, it can be indicated how ethical hacking addresses both business risk and IT risk themes, as is evident in Table 6.6.
<table>
<thead>
<tr>
<th>Business Risk</th>
<th>IT risk themes with control objectives in brackets</th>
<th>Ethical Hacking</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Physical risk</strong></td>
<td>• Unauthorised <em>(authorisation, security)</em> physical access, and lack of physical access control and security.</td>
<td>• Social engineering techniques.</td>
</tr>
<tr>
<td></td>
<td>• Theft or damage to IT equipment <em>(security)</em>.</td>
<td>• Dumpster diving.</td>
</tr>
<tr>
<td></td>
<td>• Data control weaknesses <em>(confidentiality, integrity)</em>.</td>
<td>• Wardriving.</td>
</tr>
<tr>
<td></td>
<td>• Business and IT disruption <em>(availability)</em>.</td>
<td></td>
</tr>
<tr>
<td><strong>Operational risk</strong></td>
<td>All IT risk themes and control objectives are relevant.</td>
<td>Social engineering techniques.</td>
</tr>
<tr>
<td></td>
<td><strong>Human resource risk</strong></td>
<td>Ethical hacking during SDLC.</td>
</tr>
<tr>
<td></td>
<td>All the IT risk themes and control objectives are relevant.</td>
<td>IT support process assessment.</td>
</tr>
<tr>
<td></td>
<td><strong>Technology risk</strong></td>
<td>Regular ethical hacking assessments.</td>
</tr>
<tr>
<td></td>
<td><strong>Business continuity and disaster recovery</strong></td>
<td><strong>Credit and market risk</strong></td>
</tr>
<tr>
<td></td>
<td>Business and IT disruption <em>(availability)</em>.</td>
<td>Application control weaknesses <em>(accuracy, integrity)</em>.</td>
</tr>
<tr>
<td></td>
<td><strong>Compliance risk</strong></td>
<td>Data control weaknesses <em>(authorisation, integrity)</em>.</td>
</tr>
<tr>
<td></td>
<td><strong>Reputational risk</strong></td>
<td>Lack of compliance with IT policies and procedures, legal and regulatory</td>
</tr>
<tr>
<td></td>
<td>Most IT risk themes <em>(and control objectives)</em>, when disclosed to regulators and stakeholders.</td>
<td>requirements.</td>
</tr>
<tr>
<td></td>
<td><strong>Chapter 6</strong></td>
<td>Data control weaknesses <em>(authorisation, confidentiality)</em>.</td>
</tr>
<tr>
<td></td>
<td><strong>Table 6.6 Ethical hacking addressing business risks and IT risk themes (own deduction)</strong></td>
<td>Complexity of legislation.</td>
</tr>
<tr>
<td></td>
<td><strong>Table 6.6 Ethical hacking addressing business risks and IT risk themes (own deduction)</strong></td>
<td>Achieving compliance through ethical hacking.</td>
</tr>
<tr>
<td></td>
<td><strong>Table 6.6 Ethical hacking addressing business risks and IT risk themes (own deduction)</strong></td>
<td>Knowledge of legislation.</td>
</tr>
<tr>
<td></td>
<td><strong>Table 6.6 Ethical hacking addressing business risks and IT risk themes (own deduction)</strong></td>
<td>Regular ethical hacking assessments.</td>
</tr>
<tr>
<td></td>
<td><strong>Table 6.6 Ethical hacking addressing business risks and IT risk themes (own deduction)</strong></td>
<td>Prevention of hacker incidents via remediation of security vulnerabilities.</td>
</tr>
</tbody>
</table>
From the table above it can be deduced that ethical hacking provides a comprehensive response to the threats posed by hackers and cybercriminals. Ethical hacking can be applied pervasively across an organisation, fully supporting corporate and IT governance processes.

Hacking affects various kinds of businesses. There is however one sector in the financial services industry that is particularly at risk of hacking: the banking sector. Throughout this thesis, numerous examples of banks and banking clients that have been affected have been cited. There are many reasons why the banking sector is a target, such as the technological advancement of the sector and general presence on the Internet. It is undeniable, however, that hackers target the banking sector due to the financial gains to be made from successful attacks. It is from this perspective that the South African banking sector will be briefly explored in the next chapter, as a precursor to the research to be conducted for this thesis.
CHAPTER 7

The banking sector in South Africa

7.1 INTRODUCTION

Technology is pervasive in all spheres of business and private life (ISACA, 2012b:2). The pervasiveness of technology is particularly evident in the banking industry, which has led to increased interconnectedness, driving the speed of change and increasing the complexity of operation in the banking sector (Boot, 2011:2). This complexity is further exacerbated by the size and number of clients in the banking sector. The four biggest banks in South Africa (Standard Bank, Absa, FNB and Nedbank) have an estimated 34.5 million retail accounts in 2011 and it is estimated that this figure will grow to 40 million by 2014. The four biggest banks also have 2 740 branches and 21 000 automated teller machines (hereafter ATMs). There is an increased uptake of mobile banking products and electronic channels in the South African banking sector. Legacy systems, the need for system and business integration and continued card fraud are drivers behind the four biggest banks planning to spend more than R30 billion on upgrading their IT systems and processes, from 2012 to 2014. The importance of the local banking sector is highlighted by South Africa being seen as a “gateway” to the rest of Africa, with many foreign banks returning, after having left during the apartheid years (Metcalfe, 2011:9, 11, 39). The reliance on IT also introduces significant risk.

The significance of hacker attacks on banks has already been highlighted in sections 3.5.3.5, 3.5.3.6, 3.8.6, 3.8.7, including several hacking incidents reported in the media, discussed in sections 1.1 and 3.12.2.2. Due to the dependency of the banking sector on technology, the high number of clients making use of banking products, frequent attacks by hackers on banks and their clients, the importance of local banking operations in the context of further expansion into Africa and continued international interest, the South African banking sector has been selected as the focus area for the proposed research, which will be discussed in chapter 8. This chapter provides the background to this proposed research. This chapter starts off with a short historical background of banking in South Africa. The reliance of the South African banking sector on IT will then be explored. This is followed by a short introduction to the South African banking industry, which leads into an analysis of the 16 registered banks in South Africa, by making use of the annual reports of each bank, particularly in the context of the risks and responses identified in this thesis. The results of the analysis of the annual reports are summarised and discussed. This will enable the
determination of trends regarding disclosure of: corporate governance practices; IT governance practices and King III IT governance attributes; CIO details; business risks; IT risk themes; and general responses to hacking. This will serve as a precursor to the empirical fieldwork to be conducted in the South African banking sector and will also be used as part of the discussion of the results of the planned fieldwork, as a comparison between what is disclosed versus actual practices in the banking sector.

7.2 SHORT HISTORY AND BACKGROUND OF BANKING IN SOUTH AFRICA

Banking in South Africa has a long and rich history, with the first government banking institution opening in 1783 (called the “Bank van Leening”) and the first private bank, the Cape of Good Hope Bank, in 1836. Until 1950, the banking sector was controlled by commercial banks, which did not have products on offer to the general public. During the 1950s, banks started diversifying, and merchant banks, general banks and discount houses emerged. In response, commercial banks started offering medium-term credit arrangements. The 1970s were characterised by the competition between building societies and commercial banks. To formalise the overlaps between building societies and commercial banks, the Deposit Taking Institution Act of 1991 was promulgated (Fourie, Falkena & Kok, 1999:75, 79; Nwanze, 2007:16). Despite the isolation during the apartheid years, the banking sector kept up or even surpassed the development in the international banking sector (David, 2008:13).

As early as the mid-1990s, South African banks started to focus on providing banking services in areas previously neglected during the apartheid years. International banks, which left South Africa due to disagreements with South Africa’s political views, also started returning after the new democratically elected government took office in 1994. From 1999 onwards, the South African banking industry was characterised by amalgamations of smaller banking operations into bigger banking operations (Nwanze, 2007:17). The Financial Sector Charter strongly encourages the creation of basic financial services to all South African citizens. This has led to the creation of Mzansi bank accounts, supported by the four major banks in South Africa. It provides a basic transaction product for low-income, mostly previously unbanked citizens (Orie, 2005:3). The total number of Mzansi accounts opened by the end of December 2010 was 4.6 million (The Banking Association South Africa, 2011:1). The mass market of underprivileged citizens is considered as a “major untapped market”, in both South Africa and the rest of Africa (Van Ravesteyn, 2005:8). In excess of 13
million adults in South Africa, consisting of adults located mostly in rural areas, do not have access to basic banking services (Maritz, 2011b). 

Although the South African banking scene is dominated by four banks, namely Standard Bank, Absa, First National Bank and Nedbank, the unbundling of banking products has led to other institutions also offering banking products. Competition tends to be fierce among banking competitors, who differentiate their various products based on price, customer service, product offering or unique technology (Van Ravesteyn, 2005:1, 6). Regulators do play a strategic role in the South African banking sector. For example, during the 1999 hostile takeover bid by Nedcor of the largest bank, Standard Bank, the Competition Commission of South Africa intervened and rejected the bid on the grounds that it would lead to unbalanced market power in the banking sector (Okeahalam, 2007:670). During 2005, the Absa Group was bought by the Barclays Group, further strengthening both banks’ position in the African continent as leading financial services providers (Absa, 2011). Barclays applied for regulatory approval in obtaining the majority shareholding in Absa, according to the conditions of section 37 of the Banks Act, 1990. A shareholding of less than 74% was another condition of the transaction (National Treasury RSA, 2005:1).

The financial crisis of 2007 has affected many banks internationally, yet locally banks have largely been unaffected. Llewellyn (2009:33) argues that due to South Africa’s strict exchange rules, local banks have been unable to invest significantly in international assets. He is of the opinion that South African banks follow a very traditional model of banking, limiting their ability to seek funding from wholesale markets. This view is shared by the Emerging Markets Monitor (2009:22) and the Banking Association of South Africa (2010:6), highlighting the regulatory framework, “prudent external lending practices” and a conservative fiscal policy as the underlying reasons for the resilience of the South African banking industry. The South African banking industry is therefore regarded as stable. It would require a significant event to destabilise the South African banking industry. Such a significant event could stem from many factors, but one in particular in the context of this thesis is the IT risks threatening the banking sector.

7.3 THE DEPENDENCY OF THE BANKING SECTOR ON IT

South Africa has an advanced banking infrastructure, and is regarded as a leader in the banking industry in Africa. New IT solutions are one of the most significant driving factors in
the banking industry. The South African banking sector is on par with many international banking sectors, not only in the products being offered, but also from a system and process perspective (Van Ravesteyn, 2005:7, 8). Even though South African banking developed in isolation for many years, the development of banking operations occurred at the same pace as other leading banks internationally. This is one of the reasons why international banks show an interest in South African banking operations (David, 2008:13).

Banks have to manage various business risks, as highlighted in section 4.2.3. The financial services industry and specifically the banking sector have a high dependency on IT. This dependency introduces fraud risk, such as identity theft and unauthorised payments. Furthermore, banking customers may also fall victim to cybercrime. This may lead to reputational consequences for the bank and may decrease business via electronic banking channels (Gillespie & Rasmussen, 2004:4). Banks deploy IT solutions to manage market risk and credit risk, as part of their overall IT strategy. IT also plays an important role in managing operational risk, by improving data centres, implementing identity management solutions and improving software development practices (Khanna, 2009). The ability to recover from a disaster, thereby decreasing a bank’s business continuity risk, is critically dependent on the readiness of the IT function and the ability to recover data and systems (Duke, 2011). A bank’s reputational risk could also be lowered by making use of “green” IT technology. Consumers today are more conscious of the impact of technology on the environment. By making use of more energy-efficient IT hardware, operational costs are lowered (Nelsestuen, 2009).

IT is one of the key enablers of financial services, in particular to low-income groups. Banks make use of IT to lower the operational costs required to process loans and automating credit and investment decisions. Banks opt for new technology solutions, such as online banking, cellular phones, smart cards, biometrics and other technology solutions to offer purchase, payments, withdrawal and funds transfer services to a wide range of clients (Campanaro, Kellermann & Nishiyama, 2004:17, 21). Several banks have addressed security concerns by opting for sophisticated technology solutions. They include Teba bank, Absa and Capitec, which have deployed biometric devices for client authentication (Campanaro, et al. 2004:22; Maritz, 2011a). Nedbank has introduced a new security feature, Approve-it™, which allows its clients to approve Internet banking transactions via their cell phones. The solution is superior to the current One-Time-Password being used by most banks (Nedbank Limited, 2012). Mobile banking continues to grow, offering easy access to banking services for a broad range of clients. With 35 million mobile phone users in South
Africa, it is estimated that at least 18% of South Africans are using mobile phones to transfer money. UBANK introduced a mobile banking solution in December 2010 to expand their operations in the unbanked and working-class sectors of South Africa. FNB’s eWallet mobile phone application account holders increased to half a million by April 2011 (Mochiko, 2010:14; Maritz, 2011b; Mittner, 2011:38). Another new emerging technology, Near Field Communication (hereafter NFC), will enable cashless payments via mobile phones. This will create a new payments network and could create significant competition for the banking sector, since this technology could be offered independently from the banking sector (Gunn, 2011:9). Absa will be deploying 4 000 NFC-enabled point-of-sale terminals in retail stores by the third quarter of 2012 (Vorster, 2012).

The advent of the Internet also played a significant role, particularly in the banking sector. Not only does it reduce costs; it also creates efficiency particularly for customers and increases competition among financial institutions (Madura, 2008:17). As at the end of December 2011, South Africa had an estimated 6.8 million Internet users (Miniwatts Marketing Group, 2012). It is estimated that this figure will grow to 10.9 million by 2015 (Goldstuck, 2010). The total number of South African online banking users was reported as 3.6 million during 2008 (Goldstuck & Dagada, 2009:119). Information on the total number of Internet banking users currently in South Africa is not readily available (Google, 2012). But, Absa reported that its online banking transactions reached the trillion rand mark during 2011 (ITWeb Limited, 2012). It has also been reported that Absa has approximately 1.25 million online banking customers (Leffii, 2012). Therefore, many South Africans make use of online banking. Hackers and cybercriminals would rather attack the computers of individual users making use of online banking, as opposed to the bank itself, since banks will most likely have state-of-the-art security devices, protecting them from hacker attacks. The end-user therefore becomes the soft target and the focus of online syndicates and hackers (Wanjikuu, 2009; ITNewsAfrica, 2009a).

Banking clients are increasingly demanding IT security as an integral part of banking processes (KPMG International, 2010:19). Banks have deployed client-side technologies to assist clients in protecting their own systems. Both Standard Bank and Nedbank made anti-phishing software, called Rapport, available to its clients during 2010. According to Standard Bank, 5 000 client machines were identified as being infected with 2 680 variants of viruses and 247 phishing websites have been identified. A total of 91 clients ignored the phishing website warnings issued via the software and further attempts to access the fraudulent sites were blocked. Standard Bank estimated that R3 million worth of potential fraud was averted.
in a two-week period from the launch of the software (Moodley-Isaacs, 2010). It is clear, then, that the banking sector has a dependency on IT for daily operations, enabling new business and also protecting the client’s assets and its own assets from hackers and cybercriminals. It needs to be determined whether the banking sector recognises this dependency and the risks associated with IT. The attention now turns to the South African banking sector and the disclosure of the risks and responses discussed in this thesis.

7.4 LOCAL BANKS IN THE SOUTH AFRICAN BANKING SECTOR

In 1986, the SARB opened a division which focused on the supervision of “domestic activities of banks and building societies” and started playing a leading role in the South African banking sector. The Registrar of Banks is the departmental head of the SARB, ensuring that the provisions of the Banks Act of 1990 (Act no. 94 of 1990) are carried out. The Registrar of Banks is also responsible for registration of institutions as banks. The supervision of banks calls for banks to operate within a legal and regulatory environment, which increases the effectiveness of risk management in the banking sector (Fourie, et al. 1999:59-60). The Banks Act of 1990 specifically states that “any person who wishes to conduct the business of a bank may apply to the Registrar for authorization to establish such a bank” (Republic of South Africa, hereafter RSA, 1990:Chapter III par 12.1).

The South African banking sector is a highly regulated environment and has to comply with numerous pieces of legislation and regulations, such as the Financial Intelligence Centre Act 38 of 2001, ECT Act, Basel II Accord, Know Your Customer (hereafter KYC) requirements and accounting standards (such as AC 133). All banks also have to be part the Payment Association of South Africa (hereafter PASA), as prescribed by the Banks Act. Most banks will also be part of international associations, such as Visa or Mastercard, which requires compliance with the PCI standards. Over and above this, the SARB and the JSE require of banks to comply with sound corporate governance practices (such as prescribed by King II and King III) (Powers, 2003:4-5; Van Ravesteyn, 2005:9; Bham, 2007:19-20). King III was effective for financial years from 1 March 2010, and by implication companies started disclosing their alignment with King III from financial years ending 28 February 2011 (IoD, 2010). Basel III banking regulations, the new Companies Act and the Consumer Protection Act are regulations and legislation banks have to comply with from 2011 (Ryan, 2010b:60). The Banking Association South Africa also released a new code of banking practice in 2011, which focuses mostly on regulating competition among banks (Ryan, 2010b:60).
There are 18 registered banks based in South Africa in total, two of which are currently under liquidation (Islamic Bank Limited and Regal Treasury Private Bank Limited). The 16 active operating banks are divided into 11 local and five foreign-controlled banks (listed in Table 7.1). There are also 13 registered branches of foreign banks, two registered mutual banks and 30 representative offices of foreign banks (SARB, 2012).

Table 7.1 Locally registered banks in South Africa (The Banking Association South Africa, 2010:141; SARB, 2012)

<table>
<thead>
<tr>
<th>No.</th>
<th>Registered Banks</th>
<th>Total Assets June 2010 (R million)</th>
<th>Financial year end</th>
</tr>
</thead>
<tbody>
<tr>
<td>Locally Controlled</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>The Standard Bank of South Africa Limited</td>
<td>781 947</td>
<td>31 December 2011</td>
</tr>
<tr>
<td>2</td>
<td>FirstRand Bank Limited</td>
<td>578 078</td>
<td>30 June 2011</td>
</tr>
<tr>
<td>3</td>
<td>Nedbank Limited</td>
<td>546 961</td>
<td>31 December 2011</td>
</tr>
<tr>
<td>4</td>
<td>Investec Bank Limited</td>
<td>201 501</td>
<td>31 March 2011</td>
</tr>
<tr>
<td>5</td>
<td>African Bank Limited</td>
<td>28 103</td>
<td>30 September 2011</td>
</tr>
<tr>
<td>6</td>
<td>Capitec Bank Limited</td>
<td>10 793</td>
<td>28 February 2011</td>
</tr>
<tr>
<td>7</td>
<td>U BANK (previously Teba) Bank Limited</td>
<td>3 520</td>
<td>28 February 2011</td>
</tr>
<tr>
<td>8</td>
<td>Grindrod Bank Limited</td>
<td>2 105</td>
<td>31 December 2011</td>
</tr>
<tr>
<td>9</td>
<td>Bidvest Bank Limited</td>
<td>2 340</td>
<td>30 June 2011</td>
</tr>
<tr>
<td>10</td>
<td>Sasfin Bank Limited</td>
<td>1 550</td>
<td>30 June 2011</td>
</tr>
<tr>
<td>Foreign Controlled</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Absa Bank Limited</td>
<td>663 076</td>
<td>31 December 2011</td>
</tr>
<tr>
<td>12</td>
<td>Mercantile Bank Limited</td>
<td>5 959</td>
<td>31 December 2011</td>
</tr>
<tr>
<td>13</td>
<td>Albaraka Bank Limited</td>
<td>2 638</td>
<td>31 December 2010</td>
</tr>
<tr>
<td>14</td>
<td>HBZ Bank Limited</td>
<td>2 065</td>
<td>31 December 2011</td>
</tr>
<tr>
<td>15</td>
<td>The South African Bank of Athens Limited</td>
<td>1 221</td>
<td>31 December 2010</td>
</tr>
<tr>
<td>16</td>
<td>Habib Overseas Bank Limited</td>
<td>734</td>
<td>31 December 2010</td>
</tr>
</tbody>
</table>

7.5 ANALYSIS OF THE ANNUAL REPORTS OF THE LOCALLY REGISTERED BANKS

The discussion and analysis that follows will focus on the locally registered banks and their disclosure of the risks and responses identified in this thesis with reference to their published annual reports. First of all, it will be determined whether the locally registered banks disclose corporate governance principles in their annual reports. In particular, the use of King II or King III will be highlighted. The disclosure of IT governance practices, such as the establishment of an IT steering committee, will be determined. Then the focus will turn to the disclosure of IT governance practices and in particular the requirements of King III, which include aspects such as: the board of directors taking responsibility for IT governance; defining an IT governance framework; appointing a CIO; monitoring and evaluating IT
investment and expenditure; including IT in the bank’s risk management processes; protection of information assets via information security management; and ensuring that the risk committee and audit committee assist with IT responsibilities (IoD, 2009b:83-87). Furthermore, it will be determined whether any of the generic business risks which have been identified in this thesis have been highlighted in the annual reports. An assessment of the disclosure of the IT risk themes identified in this thesis will follow, and it will also be determined whether any of the responses to hacking identified in this thesis have been disclosed.

The focus of the analysis will be on the 16 locally registered banks in South Africa (Table 7.1), which are required to publish their annual financial statements within six months after the end of the financial year (Republic of South Africa, 2008:par. 30(1)). Registered branches, mutual banks and representative offices are excluded from the analysis, given that their operations are mostly smaller in nature. At the time of writing (the week starting 22 April 2012), three banks’ annual reports for 2011 were not available yet and consequently their 2010 annual reports were used.

**7.5.1 Disclosure of corporate governance practices**

**7.5.1.1 Objective of the analysis**

The objective of the analysis is to determine whether the banks are disclosing that they are following principles of good governance and whether they are adhering to the corporate governance principles of either King II or King III.

**Table 7.2 Disclosure of corporate governance practices (own calculation from the annual reports) (n=16)**

<table>
<thead>
<tr>
<th>Corporate governance practices</th>
<th>Yes</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Following principles of good corporate governance</td>
<td>15</td>
<td>94%</td>
</tr>
<tr>
<td>Following the corporate governance principles of King II</td>
<td>2</td>
<td>13%</td>
</tr>
<tr>
<td>Following the corporate governance principles of King III</td>
<td>14</td>
<td>88%</td>
</tr>
<tr>
<td>Audit committee in place</td>
<td>16</td>
<td>100%</td>
</tr>
<tr>
<td>Risk management committee in place</td>
<td>15</td>
<td>94%</td>
</tr>
</tbody>
</table>

**7.5.1.2 Findings and deductions**

Almost all the banks (94%) disclosed in their annual reports that they prescribe to principles of good corporate governance, with the exception of UBANK Limited (hereafter UBANK), which did not have any discussion on corporate governance in their annual report. Almost all
banks (88%) have disclosed the adoption of the corporate governance code King III, with the exception of UBANK and Habib Overseas Bank Limited, which has not disclosed the use of either King II or King III. HBZ Bank and The South African Bank of Athens Limited (2010:10) referred to both King II and King III. In general, banks have adopted the new corporate governance code, King III. All the banks disclosed that they have an audit committee. All the banks, except Habib Overseas Bank, disclosed that they have risk management committees.

7.5.2 Disclosure of IT governance practices

7.5.2.1 Objective of the analysis

The objective of the analysis is to determine whether the banks are disclosing their IT governance practices, which includes aspects such as making use of an IT steering committee, prescribing to the IT governance principles recommended by King III, and determining whether CIO details are being disclosed.

7.5.2.2 Findings and deductions

Table 7.3 Disclosure of IT governance practices (own calculation from the annual reports) (n=16)

<table>
<thead>
<tr>
<th>Disclosure of IT governance practices</th>
<th>Yes</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disclosure of IT governance practices.</td>
<td>9</td>
<td>56%</td>
</tr>
<tr>
<td>Extensive discussion of IT governance practices.</td>
<td>5</td>
<td>31%</td>
</tr>
<tr>
<td>IT steering committee at board of directors level in place.</td>
<td>2</td>
<td>13%</td>
</tr>
<tr>
<td>IT steering committee at executive management level in place.</td>
<td>7</td>
<td>44%</td>
</tr>
</tbody>
</table>

From an IT governance perspective, 56% of the banks disclosed IT governance to some extent in their annual reports. This is low, considering that 88% disclosed that they prescribe to the corporate governance principles of King III. It could also be an indication that IT governance has not been established yet at some banks or that it is not important enough to disclose. Most banks only made a short reference to IT governance, without providing any further details. Only 31% of the banks provided a detailed discussion of their IT governance practices. 57% of banks indicated that they have an IT steering committee. The IT steering committees are mostly positioned at executive management level (44%), in contrast with the requirements of King III, which recommends that an IT steering committee should be established at the board of directors level (IoD, 2009b:46). In its integrated annual report, Absa Bank Limited disclosed that its IT steering committee is established at management level and that other committees, such as the audit committee and risk committees, assist
with IT governance oversight (Absa Group Limited, 2011:56). Not all banks have established an IT steering committee; however, due to the size of some of the banks, it may not be required. The fact that IT steering committees have mostly been established at executive management level indicates that IT is not yet receiving priority attention at board of directors level.

Table 7.4 Disclosure of the IT governance attributes defined by King III (own calculation from the annual reports) (n=16)

<table>
<thead>
<tr>
<th>King III IT governance attributes</th>
<th>Yes</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>The board of directors takes responsibility for IT governance.</td>
<td>7</td>
<td>44%</td>
</tr>
<tr>
<td>Define an IT governance framework applied.</td>
<td>3</td>
<td>19%</td>
</tr>
<tr>
<td>Appointed a CIO.</td>
<td>6</td>
<td>38%</td>
</tr>
<tr>
<td>Monitor and evaluate IT investment and expenditure.</td>
<td>7</td>
<td>44%</td>
</tr>
<tr>
<td>IT should be included in the bank’s risk management processes.</td>
<td>4</td>
<td>25%</td>
</tr>
<tr>
<td>Information assets protected via information security management.</td>
<td>5</td>
<td>31%</td>
</tr>
<tr>
<td>Risk committee and audit committee assist with IT responsibilities.</td>
<td>7</td>
<td>44%</td>
</tr>
</tbody>
</table>

King III has defined seven core principles as part of the governance of IT (IoD, 2009b:82-87), listed in Table 7.4 above. It is evident that there is inconsistency among banks in terms of what should be disclosed from an IT governance perspective. It is not always disclosed whether the responsibility for IT governance rests with the board of directors (44%) or not. It is also not clear whether a CIO has been appointed (38%) or not, although arguably due to the size of some of the banks, a CIO might not be required. Protecting a bank’s confidential client data should be a top priority, yet the use of information security management has been disclosed by only five banks (31%). Only 44% of the banks disclosed that their risk committee or audit committee assists with IT responsibilities. This is also an indication that IT matters are referred to other committees and might only be dealt with at a high level by the board of directors.

Table 7.5 Disclosure of the CIO’s details (own calculation from the annual reports) (n=16)

<table>
<thead>
<tr>
<th>CIO details</th>
<th>Yes</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIO’s qualifications disclosed.</td>
<td>1</td>
<td>6%</td>
</tr>
<tr>
<td>CIO’s experience disclosed.</td>
<td>2</td>
<td>13%</td>
</tr>
<tr>
<td>CIO member of the board of directors.</td>
<td>0</td>
<td>0%</td>
</tr>
</tbody>
</table>

Only one bank (Nedbank) disclosed its CIO’s qualification and only two (Nedbank and Capitec Bank) disclosed their CIOs’ experience. None of the banks have indicated whether their CIOs are members of the board of directors or not. Given that King III recommends the appointment of a CIO, it could be expected that banks will disclose whether they have appointed a CIO or not.
7.5.3 Disclosure of business risks

7.5.3.1 Objective of the analysis

The objective of the analysis is to determine whether the banks disclose any of the business risks identified in this thesis, with the purpose of understanding the importance of each of those business risks within the banking sector.

7.5.3.2 Findings and deductions

Table 7.6 Disclosure of business risks (own calculation from the annual reports) (n=16)

<table>
<thead>
<tr>
<th>Business risks</th>
<th>Yes</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance risk</td>
<td>16</td>
<td>100%</td>
</tr>
<tr>
<td>Operational risk</td>
<td>16</td>
<td>100%</td>
</tr>
<tr>
<td>Credit risk</td>
<td>15</td>
<td>94%</td>
</tr>
<tr>
<td>Market risk</td>
<td>15</td>
<td>94%</td>
</tr>
<tr>
<td>Reputational risk</td>
<td>14</td>
<td>88%</td>
</tr>
<tr>
<td>Business continuity risk</td>
<td>13</td>
<td>81%</td>
</tr>
<tr>
<td>IT risk</td>
<td>12</td>
<td>75%</td>
</tr>
<tr>
<td>Disaster recovery risk</td>
<td>10</td>
<td>63%</td>
</tr>
<tr>
<td>Human resource risk</td>
<td>6</td>
<td>38%</td>
</tr>
<tr>
<td>Technology risk</td>
<td>5</td>
<td>31%</td>
</tr>
<tr>
<td>Physical risk</td>
<td>4</td>
<td>25%</td>
</tr>
</tbody>
</table>

From a business risk perspective, all the banks highlighted compliance risk and operational risk as significant business risks in their annual reports. Credit risk and market risk have been highlighted by almost all the banks (94%), followed by reputational risk (88%) and business continuity risk (81%). The definition of operational risk has been defined as people, processes, systems and external events by 14 (88%) banks. It is not clear from this disclosure, however, whether the systems component refers to IT or not. Only one bank (UBANK) has substituted the term “system” with “IT” in its annual reports, which implies that IT risk is managed as a component of operational risk (UBANK, 2011:22). Furthermore, only 75% of the banks highlighted IT risk as a key business risk in their annual report, despite the fact that all the banks are by necessity highly dependent on IT. Technology risk has only been highlighted in 31% (4 out of 16) of the annual reports. Physical risk has only been disclosed by some banks (25%), despite the fact that the physical protection of IT systems should be of primary consideration to banks.
7.5.4  Disclosure of IT risk themes

7.5.4.1  Objective of the analysis

The objective of the analysis is to determine whether the banks disclose any of the IT risk themes identified in this thesis (section 4.3.5.17), with the purpose of understanding the importance of each of those IT risk themes within the banking sector.

7.5.4.2  Findings and deductions

A few specific risks (all part of cybercrime) have been added to the existing IT risk themes, specifically phishing, hacking and insider attacks to determine whether those are being disclosed or not, seeing that cybercrime is such a broad IT risk. The IT risk themes which will be used later as part of the questionnaires, have been abbreviated and are displayed here in brackets to facilitate the comparison of the results presented in chapter 9.

Table 7.7  Disclosure of IT risk themes (own calculation from the annual reports)  
(n=16)

<table>
<thead>
<tr>
<th>IT risk themes (taken from Table 4.25)</th>
<th>Yes</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business and IT disruption. (IT continuity risk)</td>
<td>16</td>
<td>100%</td>
</tr>
<tr>
<td>Lack of segregation of duties.</td>
<td>7</td>
<td>44%</td>
</tr>
<tr>
<td>Unauthorised physical access / lack of physical access control and security. (Physical access risk)</td>
<td>5</td>
<td>31%</td>
</tr>
<tr>
<td>Inadequate change / project management practices. (Lack of software development)</td>
<td>4</td>
<td>25%</td>
</tr>
<tr>
<td>Data control weaknesses. (IT systems risk)</td>
<td>4</td>
<td>25%</td>
</tr>
<tr>
<td>Lack of compliance with IT policies and procedures, legal and regulatory requirements. (IT non-compliance risk)</td>
<td>3</td>
<td>19%</td>
</tr>
<tr>
<td>Inadequate IT operations and support.</td>
<td>3</td>
<td>19%</td>
</tr>
<tr>
<td>Misuse of IT / irregularities and fraud.</td>
<td>3</td>
<td>19%</td>
</tr>
<tr>
<td>Inadequate IT performance.</td>
<td>3</td>
<td>19%</td>
</tr>
<tr>
<td>Theft or damage to IT equipment. (Physical access risk)</td>
<td>2</td>
<td>13%</td>
</tr>
<tr>
<td>Cybercrime.</td>
<td>2</td>
<td>13%</td>
</tr>
<tr>
<td>Unauthorised logical access. (Logical access risk)</td>
<td>2</td>
<td>13%</td>
</tr>
<tr>
<td>Interface control weaknesses. (Communication failure)</td>
<td>2</td>
<td>13%</td>
</tr>
<tr>
<td>Phishing (Cybercrime)</td>
<td>1</td>
<td>6%</td>
</tr>
<tr>
<td>Complexity of IT.</td>
<td>1</td>
<td>6%</td>
</tr>
<tr>
<td>IT human resource deficiencies. (IT human resources risk)</td>
<td>1</td>
<td>6%</td>
</tr>
<tr>
<td>Application control weaknesses. (IT systems risk)</td>
<td>1</td>
<td>6%</td>
</tr>
<tr>
<td>Operating system weaknesses. (IT systems risk)</td>
<td>1</td>
<td>6%</td>
</tr>
<tr>
<td>Hacking (Cybercrime)</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Insider attacks (Cybercrime)</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Inefficient use of IT resources.</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Lack of an audit trail.</td>
<td>0</td>
<td>0%</td>
</tr>
</tbody>
</table>

It is evident that disclosure of specific IT risks is minimal amongst banks, with business and
**IT disruption** the only risk mentioned by all the banks (100%). **Lack of segregation of duties** (44%) and **unauthorised physical access** (31%) are mentioned by a few banks. In section 3.12.6 it has been highlighted that the fear for reputational consequences may lead to non-disclosure of hacking incidents. Despite the interest in hacking and other cybercrime incidents by the public in general, almost none of the banks have highlighted this as a key concern. Only Investec disclosed some information closely related to the risk of hacking: “We may be vulnerable to the failure of our systems and breaches of our security systems” (Investec, 2011:38). In fact, it is difficult to determine whether the banks have responses in place to protect themselves against hacking and cybercrime. In general, only a few IT risk themes have been disclosed in the annual reports. Considering the dependency of the banking sector on IT, it is debatable whether there is enough focus on IT risk in the annual reports.

### 7.5.5 Disclosure of general responses to hacking

#### 7.5.5.1 Objective of the analysis

The objective of the analysis is to determine whether any of the responses to the hacking identified and discussed in section 5.2 of this thesis are being disclosed in the annual reports. A few responses have been added: security technologies, governance frameworks and software development practices, to allow for a more granular identification of responses disclosed in the annual reports. The list of responses will also be used as part of the questionnaires.

#### 7.5.5.2 Findings and deductions

<table>
<thead>
<tr>
<th>Disclosure of general responses to hacking</th>
<th>Yes</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal control</td>
<td>16</td>
<td>100%</td>
</tr>
<tr>
<td>Risk management</td>
<td>16</td>
<td>100%</td>
</tr>
<tr>
<td>Corporate governance</td>
<td>15</td>
<td>94%</td>
</tr>
<tr>
<td>IT governance</td>
<td>10</td>
<td>63%</td>
</tr>
<tr>
<td>Enterprise risk management (ERM)</td>
<td>6</td>
<td>38%</td>
</tr>
<tr>
<td>Information security management</td>
<td>5</td>
<td>31%</td>
</tr>
<tr>
<td>Software development practices</td>
<td>1</td>
<td>6%</td>
</tr>
<tr>
<td>Governance frameworks, such as CoBiT</td>
<td>1</td>
<td>6%</td>
</tr>
<tr>
<td>Applying service and quality management, such as ITIL</td>
<td>1</td>
<td>6%</td>
</tr>
<tr>
<td>Ethical hacking</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Security technologies, such as firewalls</td>
<td>0</td>
<td>0%</td>
</tr>
</tbody>
</table>
All the banks have disclosed the responses *internal control* and *risk management*, which are conventional responses required from a corporate governance perspective. This is closely followed by corporate governance (94%). Only 38% of the banks indicated that they are following extended risk management practices through ERM. IT governance has only been disclosed in 63% of the annual reports. The banks have not disclosed their use of best practice frameworks, with the exception of Capitec, which disclosed that it is using CobiT, ITIL and ISO 27001 (Capitec Bank Holdings Limited, 2011:67). It is also an indication that most banks might not be using best practice frameworks. Ethical hacking and security technologies have not been disclosed by any of the banks.

### 7.6 CHAPTER SUMMARY

The chapter opened with a brief introduction of the history and background of banking in South Africa. This was followed by a discussion of the dependency of the South African banking sector on IT, as a precursor to the discussion of the registered banks in South Africa. The annual report of each of the 16 registered banks was analysed, with specific reference to the disclosure of the risks and responses identified in this thesis.

The analysis of the annual reports indicated that the banking sector is generally consistent in disclosing corporate governance principles, taken mostly from King III. From the perspective of the business risks identified in this thesis, compliance risk, operational risk, credit risk, market risk and reputational risk are key risks disclosed in the annual reports. It is surprising that IT risk has not been disclosed as a key business risk by all banks. Hacking as a risk has also not been disclosed by any of the banks.

IT governance has been disclosed in the annual report of most banks, mostly without any elaboration on the key components of IT governance. There is also minimal disclosure of the IT risk themes identified in this thesis, which poses the question about how the banking sector manages and mitigates IT risks.

The information available to investors and the general public does not provide enough insight into how the banking sector manages and mitigates IT risk and the risk of hacking in particular. If anything, it would actually create doubt and uncertainty as to the banking sector’s ability to mitigate these risks. This then forms the basis of the fieldwork to be conducted in the banking sector, since clarity is required on how significant IT risk and
hacking in particular are considered within the banking sector and how the banking sector responds to these risks.
CHAPTER 8
Research Methodology

8.1 INTRODUCTION

The first six chapters of this thesis presented information on hacking and the governance responses thereto by using an extensive literature review. The disclosure of the risk of hacking and responses thereto were assessed by way of an analysis of the annual reports of registered banks in South Africa was presented in chapter 7. Following on from this analysis, this chapter will not only reflect on the two questionnaires applied in the banking industry in South Africa as the fieldwork for this thesis, but will also consider the three research methodologies: literature review, analysis of the annual reports of the locally registered banks in South Africa and application of the questionnaires.

8.2 LITERATURE REVIEW

Briefly, the objective of a literature review is to engage with the established literature in order to determine the extent of the available body of knowledge and research, while avoiding merely echoing the conclusions reached by other scholars (Bryman & Bell, 2007:95, 107). It also aids in the formulation and refinement of research questions and assists with the identification of research possibilities (Gill & Johnson, 2006:25). The literature review presented in Chapters 2 to 4 established the theoretical stance on IT risk within the context of business risk and its close association with the risk of hacking. A wide range of sources was consulted as part of the literature review, including governance, auditing, information security and other IT sources. The literature review continued in Chapters 5 and 6, which explored the possible responses that could be applied by the board of directors to the risk of hacking. These chapters ultimately argued that ethical hacking is an effective response to the risk of hacking.

Based on the literature review, thematological questions were formulated in each chapter. These thematological questions were posed to prioritise the analysis of the annual reports and in the design of the questionnaires described later on in this chapter.
8.3 ANALYSIS OF THE ANNUAL REPORTS OF LOCALLY REGISTERED BANKS IN SOUTH AFRICA

Based on the literature review performed and set out in Chapters 2 to 6, this study also presented the results of a focused analysis of the annual reports of the registered banks in South Africa.

The analysis set out to determine whether the locally registered banks in South Africa disclose information that provides shareholders, investors and stakeholders with insight into how governance responsibilities towards managing and mitigating IT risks (such as hacking) are discharged. Several aspects could be indicators of this responsibility, such as the disclosure of significant business risks, IT risks, corporate governance and IT governance practices. It was also necessary to establish which responses to IT risks, such as hacking, are disclosed. The process followed during the analysis was to review each bank’s disclosure of the aforementioned aspects in its latest available annual report, by systematically analysing the items being disclosed. The results of the analysis were summarised and presented in Chapter 7. The results indicated the lack of disclosure of IT risk and responses to IT risk, as well as inconsistencies in the disclosure of IT governance practices. This indicates the need to clarify these governance responsibilities and responses to hacking as part of the questionnaires sent out to the locally registered banks.

Therefore, further research must be conducted to determine the level of responses of the boards of directors at the locally registered banks in South Africa to IT risk and specifically the risk of hacking. This empirical research will take the form of two questionnaires that will seek to determine:

1. What the responses to hacking are in the South African banking sector.
2. What the depth of the governance responses to hacking is in the banking sector.
3. Whether the board of directors provides sufficient oversight and focus on IT risk.
4. Whether hacking is considered a threat in the banking sector.
5. The extent to which banks make use of ethical hacking as a possible response to the threat of hacking.
8.4 QUESTIONNAIRES

The final step in achieving the objectives of this study was to administer two questionnaires to the appropriately placed employees of the locally registered banks in South Africa. Research conducted by using questionnaires is considered very reliable, given that the fieldwork can be replicated through repeating the same questions to the same population of participants (Sumser, 2001:162). This approach was indeed followed: a generic questionnaire for each of the two groups of respondents targeted in the local banking sector was compiled using a mixed-method approach. Mixed method research involves a mixture of both quantitative and qualitative research approaches, and attempts to achieve a more comprehensive understanding of the research problem (Creswell & Plano Clark, 2007:5; Creswell, 2009). More emphasis was placed on the quantitative approach, while open-ended questions provided qualitative data to enrich and expand the research results (Morse & Niehaus, 2009:14; Creswell & Plano Clark, 2007:11).

Quantitative research focuses on the study of “natural phenomena” by using research methods such as surveys, laboratory experiments and numerical methods (Ohwobete, 2009:15). In particular, organisational practices could be determined via quantitative questionnaires. Quantitative methods involve the process of collecting, scrutinising, interpreting and presenting numerical information (Teddlie & Tashakkori, 2009:5). Quantitative research involves the collection and analysis of data in order to establish the relationships between the theory and research, with an emphasis on testing the theories (Bryman & Bell, 2007:28). The research questions used as part of the quantitative research approach provide a means of guiding the researcher towards discovering unknown facts (Teddlie & Tashakkori, 2009:5). In this study, these unknown facts were established via quantitative research questionnaires sent to two distinct groups in the South African banking sector, covering corporate governance, IT governance, risk management and ethical hacking practices. The quantitative results provide data which can be analysed in order to highlight distinct trends within the local banking sector regarding responses to hacking.

Quantitative research can be used to generalise the findings beyond the selected participants. The sample needs to be representative to allow for generalising to the rest of the population (Saunders, Lewis & Thornhill, 2007:120; Bryman & Bell, 2007:169). It is at least possible to generalise the findings to the non-responding participants in the local banking sector, other smaller banking operations in South Africa and possibly also to other South African financial service operations offering similar products and services to banks.
Qualitative research seeks to gather detailed data in order to build a deeper understanding of the research problem (Cooper & Schindler, 2006:198). Qualitative research is used to study “social, cultural and organizational phenomena” (Ohwobete, 2009:15). The responses can be insightful, in-depth and even unexpected (Mack, Woodsong, MacQueen, Guest & Namey, 2005:4). The questionnaires in this thesis have specifically been designed to include a general comments question at the end of each section, which allowed respondents to add qualitative comments regarding the questions answered. The qualitative comments provided valuable insight into the practices followed by some of the banks, although generally the comments received from participants were of a limited nature.

8.5 DEFINING THE POPULATION AND STRATA FOR THE APPLICATION OF THE QUESTIONNAIRE

The focus of this part of the research was on two homogeneous groups of individuals in the local banking sector of South Africa, more specifically the company secretary and the individual responsible for IT at each of the 16 locally registered banks, as presented in Table 7.1. All 16 locally registered banks as at December 2011 have been selected as the target group. The intention was to obtain a wide range of views from the local banking sector and consequently a census approach was followed by contacting all the banks (Marx & Voogt, 2010:25). The target population of two distinct groups therefore consists of 32 potential participants. Given the exploratory nature of this study and the general lack of knowledge about IT governance practices, IT risk and hacking in the local banking sector, general trends and similarities between the two groups were sought.

The size of the population is small, but the South African banking sector, while very dynamic and competitive, has only a few role-players. Targeting small populations is not uncommon in doctoral studies. The South African banking sector was targeted by Young in his doctoral study on operational risk management, although he targeted more respondents at each bank (Young, 2001:240). Al-Azazi targeted 19 participants in his study on the information security assessment of e-governments in Dubai (Al-Azazi, 2008:121). In the research conducted by Bédard and Gendron (2004:195), only three out of 17 public companies (18%) agreed to participate in their research project (Bédard & Gendron, 2004:195). De Haes targeted 22 experts in his study on the implementation of IT governance in the Belgian financial services sector (De Haes, 2007:128). Therefore, the total population group of 32 potential participants used in the present study can be regarded as sufficient in the context of this study.
8.5.1 Company secretaries as the target group

The appointment of a company secretary is mandatory for all public and state-owned companies under the Companies Act (RSA, 2008: section 84, section 86), and these secretaries have an indispensable role to play in terms of corporate governance in the organisation. The company secretary holds a key position in the organisation, has to be a trusted advisor and an individual with good character and business acumen to ensure that the board of directors adheres to principles of good corporate governance and ethics (Financial Reporting Council, 2006:A.5.3; Van Schalkwyk, 2007:17; Institute of Chartered Secretaries and Administrators, hereafter ICSA, 2012; South African Law School, 2010; Al Baraka Bank, 2010:19). According to Van Schalkwyk, from time to time the company secretary may be a member of the executive committee. He or she should not be directly involved in decision-making, but will indirectly influence the decisions made by the board of directors (Van Schalkwyk, 2007:14, 19). The JSE requires the company secretary to have an “arm’s-length relationship” with the board of directors, and he or she should ideally not be a director (JSE, 2012:1). Many company secretaries will be members of the Chartered Secretaries of South Africa, which sets out as its mission to be “the leading advocate of governance best practices in the private and public sectors in Southern Africa” (Chartered Secretaries South Africa, hereafter CSSA, 2012).

The company secretary has to protect the interests of the company (Wolpert, 2011:5). He or she assists with the appointment of directors and also needs to ensure that the board of directors and other committee charters are up to date and relevant in terms of current corporate governance practices (Du Plessis, 2012:5). The company secretary also has to ensure the independence of the board of directors in order to enable them to provide clear direction to the organisation (Van Schalkwyk, 2007:15). The board of directors has to establish reporting lines for the company secretary, ensure that the company secretary’s position is protected and support the company secretary in his or her role. All directors have access to the services and advice of the company secretary (The Committee on the Financial Aspects of Corporate Governance and Gee and Co. Ltd. 1992:4.25; Wolpert, 2011:1; Investec, 2011:223).

Company secretaries have various legislative duties, such as ensuring that directors are aware of any laws relevant to the company, that all shareholder and board meeting minutes have been properly recorded, that statutory deadlines are met and that the annual financial statements of the organisation have been sent to everyone entitled to receive them (Van Schalkwyk, 2007:17; RSA, 2008: section 88(2); South African Law School, 2010).
company secretary is also responsible for communication with the shareholders. This includes communicating the organisation’s governance practices in the integrated annual report and acting as the primary contact point for stakeholders (Van Schalkwyk, 2007:20; Wolpert, 2011:6).

A company secretary plays a key role in defining the organisation’s corporate governance practices. He or she has to advise the board of directors on its corporate governance responsibilities and also assists in setting the agenda of work for the year that lies ahead for the board of directors and all other board committees (Matisonn & Armstrong, 2012; IoD, 2009b:43-44;). The company secretary has a close working relationship with the chairman of the board of directors. It is advisable that the chairman of the board meet with the company secretary, the CEO and/or the CFO before board meetings to cover significant issues and agree on the agenda (Van Schalkwyk, 2007:10; IoD, 2011:4; Wolpert, 2011:9; Investec, 2011:224). The company secretary enhances the effectiveness of the board of directors by ensuring that pivotal information is made available to it in order for it to carry out its corporate governance responsibilities (Van Schalkwyk, 2007:16; Walker, 2009:23). The company secretary facilitates the flow of information between management and the board of directors (Maltas, 2000:74; Financial Reporting Council, 2006:A.5; Capitec, 2011:42). Furthermore, the company secretary has to be in touch with the latest developments in the "corporate governance landscape" in order to provide pre-emptive warnings about issues that may affect the accountability of board of directors (Wolpert, 2011:5). This will include the responsibility of ensuring adherence to the requirements of King III.

The company secretary also has to advise and assist the board of directors with its risk management responsibilities. He or she needs a thorough understanding of risk management practices and have to be familiar with the risk types prevalent in the industry and in the organisation in particular. This includes an understanding of risks associated with information systems and new technology (Wolpert, 2010:37). The company secretary also needs to be familiar with audit, internal control and the effective functioning of the audit committee (ICSA, 2008:3; Smyth-Faulker, 2010). The company secretary is responsible for identifying the training needs of directors, in particular from a corporate governance perspective (IoD, 2009b:43; Wolpert, 2011:4; FirstRand, 2011:69). This also implies that the company secretary will have a good working knowledge of governance practices being followed in his or her respective organisation, as well as the potential gaps that may exist.

Given the corporate governance responsibilities of company secretaries, the fundamental role they play in an organisation and their close interaction with the board of directors, they
have been selected as participants in the empirical research. They can provide valuable insights into the inner workings of the board of directors and the supporting committees and also have access to meeting minutes and board packs.

8.5.2 Individuals responsible for IT as the target group

The importance of IT in today’s business world has been highlighted in King III with the introduction of IT governance. The significance of IT governance as a component of corporate governance is emphasised by its inclusion in King III: “The pervasiveness of IT in business today mandates the governance of IT as a corporate imperative” (IoD, 2009b:16). Core components of IT governance are IT risk governance and IT value governance. This closely integrates IT governance with corporate governance (Parent & Reich, 2009:138). The strategic nature of IT in many organisations has led to the appointment of an individual to oversee this function. King III encourages the appointment of a CIO, whose duty is to interact with both the business and the board of directors on strategic IT and IT governance matters (IoD, 2009b:84). The CIO of today is required to demonstrate returns on IT investments and ensure that IT is contributing to the organisation’s overall performance. This can only be achieved through greater transparency and when IT clearly aligns with corporate business objectives (Morton, 2012:1, 7). The CIO therefore also becomes an enabler of business performance. The CIO makes use of IT governance to ensure technology resources are directed at achieving business goals. Furthermore, IT governance includes responsibilities such as IT risk management and information security (Posthumusa & Von Solms, 2005:12; Ban, Cocchiara, Lovejoy, Telford and Ernest, 2010:1). In particular, the CIO’s IT risk management responsibilities are on the increase. Effective IT risk management practices will contribute to the overall business objectives of the organisation. IT risk capabilities should focus on risks across the organisation, including risks pertaining to data, security, resilience, disaster recovery and new technology (Ban, et al. 2010:1, 10). It is from this perspective that the CIO will have significant insight into IT governance and the management of IT risks, such as hacking. Although not all banks are big enough to warrant the appointment of a CIO, a specific individual should be given the responsibility of managing the IT function. This group will provide valuable insight into the IT risk, IT governance and ethical hacking practices followed at each bank. The CIO has also been identified as a common role-player in many of the responses to hacking discussed in sections 5.5.4, 5.9.7 and 6.13. As far as the responses to IT risk are concerned, as well as the use of ethical hacking, the individual responsible for IT will be in a good position to provide the required insight into IT governance, IT risk and ethical hacking and therefore the second questionnaire was sent to the individuals responsible for IT.
8.6 DESIGN OF THE QUESTIONNAIRES

The mixed-method research was delivered to the two groups of participants by means of questionnaires, which contained measurement questions and general comments sections. The measurement questions and statements in the two questionnaires were derived from the thematological questions presented throughout the literature review, discussions with academics and consideration of issues that were pertinent at the time. Each question or set of statements were considered carefully, and often shortened and simplified to ensure that the questionnaires were comprehensible and not too lengthy to complete. In most cases, respondents were asked to use a Likert scale to answer the questions, or were simply required to answer yes or no. Ranking of statements was also used in a few instances. Statements used in the questions were listed randomly to avoid potential bias (Voogt, 2010:85). A general comments section was added to each section as the qualitative component of the questionnaire, to allow the respondents to clarify answers or provide additional comments. The questionnaires were developed in Microsoft Word, with the forms fill-option-enabled and restricted editing protection enforced. The questionnaires were also made available online on a specially developed web-site. The functionality for the online questionnaires was more flexible and allowed for the mandatory completion of each question. A token was built into the URLs in order to allow for tracking of the participants. Therefore, a unique URL was made available to each of the 32 participants. The questionnaires were delivered via surface mail, email and in a few instances hand-delivered. Participants had the option of completing the questionnaire online, electronically or manually and returning them via return surface mail (a stamped, self-addressed envelope was provided), email or fax. A few surveys were hand-collected.

8.6.1 Design of the company secretary questionnaire

The company secretary questionnaire appears in Annexure A. The following themes were the focal points for the company secretary questionnaire:

- **Question 1** was aimed at asking supporting opening questions about the company secretary’s corporate governance role.
- **Question 2** was aimed at establishing the IT governance responsibilities of the board, from the company secretary’s perspective.
- **Question 3** was aimed at determining the significance of IT within the business context, from the company secretary’s perspective.
- **Question 4** was aimed at establishing what drives the incorporation of IT governance
in the organisation.

- **Question 5** and **question 6** were aimed at asking specific questions about the individual responsible for IT, also in an effort to establish the relative position of the individual in the organisation, as an indication of the importance of IT. The individuals’ contact details were also obtained.

- **Question 7** was aimed at establishing to what extent the board of directors and board committees deal with IT matters.

- **Question 8** was aimed at determining the extent of the link between IT risk and a number of business risks.

- **Question 9** and **question 10** were aimed at establishing how hacking would increase a number of IT risks. Furthermore, the extent and effectiveness of general responses to hacking were determined.

- **Question 11** was aimed at establishing IT governance disclosure practices in the organisation.

### 8.6.2 Design of the individual responsible for IT questionnaire

The individual responsible for IT questionnaire is recorded in Annexure B. The following themes were the focal points for the individual responsible for IT questionnaire:

- **Question 1** was aimed at asking supporting opening questions about the individual responsible for the IT governance role.

- **Question 2** was aimed at establishing the IT governance responsibilities of the board, from the perspective of the individual responsible for IT.

- **Question 3** was aimed at determining the significance of IT within the business context, from the perspective of the individual responsible for IT.

- **Question 4** was aimed at establishing what drives the incorporation of IT governance in the organisation.

- **Question 5** was aimed at determining the extent of the link between IT risk and a number of business risks.

- **Question 6** and **question 7** were aimed at establishing the significance of hacking in the organisation and how it will increase a number of IT risks. Furthermore, the extent and effectiveness of general responses to hacking were determined.

- **Question 8** was aimed at establishing the ethical hacking practices in the organisation.

- **Question 9** asked for some specific details about the qualifications and experience of the individual responsible for IT.
8.7 PILOT STUDY

A pilot study was conducted before the questionnaires were distributed. Pilot research is defined as “a trial run-through to test the research design with a subsample of respondents who have characteristics similar to those identifiable in the main sample to be surveyed”. This will assist with eliminating any ambiguities that may exist in the questions (Gill & Johnson, 2006:120-121). The pilot study further ensures the validity and clarity of the questions (Sanchez, 2010:10), allowing the researcher to update questions, before using them during the actual fieldwork. The participant can be asked during the pilot study to comment on the attributes of validity and clarity (Sanchez, 2010:10).

It was decided that an electronic document version of the questionnaire and a web-based version of the questionnaire would be made available to all participants in the pilot study. As part of the pilot study, the questionnaires in Microsoft Word format and an accompanying URL to the website were tested by academic staff lecturing in governance and auditing in the University of Johannesburg’s Department of Accountancy. The questionnaires were also completed by internal audit specialists at two of the largest banks in South Africa. Comments and recommendations could all be accommodated in the questionnaires. Comments included clarification regarding less familiar terminology, such as “hacking” and “cybercrime”. Definitions were added to the phrasing of the questions. There were also comments regarding the order of the Likert scale. The presentation of the Likert scale was adjusted to ensure all started with the most positive rating and ended with the most negative rating.

8.8 DATA COLLECTION, ANALYSIS AND RETENTION

In this thesis, a census approach was followed to obtaining responses from all the identified participants in the banking sector. A critical step in the research is the data-collection process followed. Data was collected through a self-administration approach, since respondents were considered well-educated and competent enough to complete the questionnaire without personal assistance. Some of the disadvantages in completing a self-administered questionnaire are that the interviewer is not present while the questionnaire is being completed, to ensure that the questions are correctly completed and that all the questions are completed. It is also not possible to prevent someone other than the intended recipient from answering the questions (Fowler, 2009:82). However, as explained in section 8.4, the surveys were addressed and followed up with particular recipients to ensure completion by the intended recipients.
Consideration was given to the delivery method of the questionnaires. One of the delivery mechanisms for quantitative research questionnaires is postal or surface mail. The advantages of using surface mail to distribute questionnaires are that the relative cost is low, surface mail can reach a distant group of participants and the participant is provided with ample time to respond to the questionnaire (Fowler, 2009:82). The response rate to questionnaires delivered by mail could be low for several reasons, such as having the incorrect postal address or the mail may be intercepted by a third party (Bless & Higson-Smith, 1995:112; Fowler, 2009:82). In this study, a few of the registered mail items remained undelivered. In the process of collecting data, a letter containing the questionnaire might be thrown away or a telephone call might be ignored. Face-to-face data collection tends to deliver a high response rate, since it is more difficult for people to ignore the researcher (Sumser, 2001:182). Web surveys are in some cases regarded as an effective means of delivering surveys. However, the lack of personalisation might affect the success of web surveys. A disadvantage associated with conducting surveys via email is that they may be considered as spam. Completion of web surveys could be encouraged by a pre-notification via surface mail (Kaplowitz, Hadlock & Levine, 2004:101). Another disadvantage is that accurate email addresses of the recipients are required (Fowler, 2009:83). The exact preference for mode of delivery to the target population was unknown. Therefore, a mixed method of surface mail and email notifications, with options to complete via a web survey, electronic Microsoft Word document or hardcopy survey were made available to all participants.

The process of data collection by means of survey questionnaires, which were mailed (surface mail) and emailed to the company secretary of each of the 16 locally registered banks commenced between the period 5 to 12 December 2011. The company secretaries were asked to provide the contact details of the individual responsible for IT. The questionnaires to the individuals responsible for IT were subsequently mailed and emailed to the individual responsible for IT during the period 6 to 12 December 2011. At first, the questionnaire was sent to only the 12 individuals responsible for IT, until further accurate contact details were obtained. As a result of the pending holiday period, the due date for the return of the questionnaires was set as 15 January 2012 for the company secretaries and 31 January 2012 for the individuals responsible for IT. Both dates were later extended to the end of February 2012. Hard-copy letters and questionnaires were also sent via registered post shortly after the emails were sent out, therefore serving as a follow-up to the first request to the 28 participants where contact details were available.

Several methods of follow-up were used to obtain responses:
Follow-up emails were sent to participants on 10 January 2012. A further six responses were subsequently received. Up to six email reminders had to be sent to selected participants during January and February 2012.

Follow-up phone calls were made to a number of non-responding participants on 23 January 2012. Further contact details were obtained. This method of follow-up did not result in any additional responses.

Follow-up surface mail was sent to nine participants on 24 January 2012, where registered letters were undelivered or new contact details were obtained.

Physical visits to 10 non-responding banks in Johannesburg and Durban were made on 28 January and 3, 10 and 17 February 2012. The physical visits produced 11 further responses. Although the physical visits were time-consuming and costly, they proved to be an effective way of obtaining non-responsive participants' buy-in and commitment to completing the questionnaire.

None of the questionnaires were returned via fax. Five questionnaires were returned via post. Six respondents completed the questionnaires online. Nine were returned via email, with four respondents completing the Microsoft Word document and five returning a scanned copy of the manually completed questionnaires. Five questionnaires were collected from the respondents themselves. The manual completion of the questionnaires was therefore the preferred method of completing the questionnaires.

Data analysis was applied to the empirical fieldwork results presented in Chapter 9. Sanchez (2010:71) described the purpose of data analysis as follows: “The data analysis requires the reduction of data, analysis of themes, and investigation of meaningful units of information related to the study’s purpose.” To complement the results, selected descriptive statistics, such as mean and standard deviation, were applied (Emory & Cooper, 1991:472-473). The mean is not commonly used in skewed distributions and therefore the weighted arithmetic mean has been calculated, to determine the relative importance of items (Voogt, 2010:85). Although the weighted arithmetic mean is meaningful for larger populations, it was nonetheless used to rank the results of some of the questions. The results of the analysis are presented in Chapter 9. Data will be retained for a period of three years. Participants were assured of the confidential treatment of the data.

Primarily two Likert scales were used by participants to rank the use of the general responses to hacking. The four-point Likert scales contained the following scales: 1 = To a large extent; 2 = To a moderate extent; 3 = To a small extent; 4= Not at all. The five-point
Likert scales contained the following scales: 1 = To a large extent; 2 = To a moderate extent; 3 = To a small extent; 4 = Not at all; 5 = Do not know. For purposes of the weighted arithmetic mean calculation, weightings were awarded in reverse order, to ensure that the response “To a large extent” carries the highest weighting (for example, for the four-point Likert scale, the scale 1 would carry a weighting of 4). The weighted arithmetic mean and mean calculations produce similar results, however seeing that different weightings have been awarded to the weighted arithmetic mean calculation, the results are different. The standard deviation and mean were calculated on the raw data captured from the questionnaires and the weighted arithmetic mean was calculated from the counts reflected in each table. Where necessary, the results were ranked in descending order according to the weighted arithmetic mean.

8.9 RESEARCH CONTROL

The respondents targeted in this research were considered to be professional individuals who would be able to complete the questionnaires without any assistance and would also take the responsibility to complete the questionnaires accurately. Data collected via the online questionnaires were captured electronically and made available in Microsoft Excel by the web administrator, and there was no need to recapture the data again. Questionnaires received via email or post, or collected physically, were captured by the researcher and independently verified by a senior forensic auditor. The results for each table were calculated by using Microsoft Excel formulas to ensure accuracy.

8.10 PROBLEMS ENCOUNTERED DURING THE STUDY

There were no significant problems during the preparation of the questionnaires. An accurate list of contact details was not available before the distribution of the questionnaires. Company secretary details were mostly obtained from each of the banks’ annual results. The email addresses, however, were not always available. Email addresses were sometimes obtained by searches on the Internet or by contacting each bank.

The CIO or head of IT details were harder to find. Again, some could be obtained by doing searches on the Internet. Others were provided by the company secretary or by doing enquiries at each of the banks. Therefore, there was a small delay in distributing the surveys to some participants. A few registered mail letters were undelivered, even though they were
personalised. These were followed up by surface mail, seeing that one participant complained about having to collect the registered mail at the post office.

A total of two individuals responsible for IT indicated that were not able to participate in the survey. One head of IT wrote an extensive email, citing reasons why he or she could not participate, pointing out in particular that he or she felt the information requested was of a sensitive nature and would expose the organisation to risk. In contrast, most company secretaries were willing to participate.

It was also clear from the physical visits to the banks (a few surveys were delivered by hand and collected by hand) that all of the selected participants were extremely busy individuals, hence finding the time to complete the surveys was a challenge. The personal assistants or secretaries of some participants were at times instrumental in ensuring that the surveys were completed.

8.11 RESPONSE RATE

There are no studies comparable to this thesis that could be used to set a benchmark for expected response rates. Marx indicated that response rates for audit committee surveys varied between 5% and 61% (Marx, 2008:356). Marx also indicated that questionnaire response rates tend to be relatively low in South Africa, ranging between 25% to 38% (Marx, 2009:31). In a study conducted by Chibayambuya on holistic risk management in the local banking sector (including foreign-controlled banking operations and multiple possible respondents at each bank), a response rate of 37% was achieved (Chibayambuya, 2007:4-139). In a study conducted by Turner on the subject of information security technology used in the US domestic banking sector, only 35 banks (42 surveys) responded to questionnaires sent to at least 3000 banks (1.17% response rate). It took Turner six months to obtain these responses. In his study, there was a general reluctance by participants to share the banks’ security technology practices, for fear that it may be used against them (Turner, 2009:93, 121). A similar reaction might have been expected from the banks in South Africa, but on the whole a high response rate was achieved.
### Table 8.1 Breakdown of survey responses to the company secretaries and individuals responsible for IT (own calculation)

<table>
<thead>
<tr>
<th>Response category</th>
<th>Questionnaire A (Company Secretaries)</th>
<th>Questionnaire B (Head of IT / CIO)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Number</td>
<td>%</td>
</tr>
<tr>
<td>Completed and usable questionnaires</td>
<td>15</td>
<td>94%</td>
</tr>
<tr>
<td>No response received</td>
<td>1</td>
<td>6%</td>
</tr>
<tr>
<td>Correspondence received – cannot participate due to internal policy</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Correspondence received – believe information is too sensitive to disclose</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td><strong>Total and percentage of questions sent out</strong></td>
<td><strong>16</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

Confirmation was received from one of the smaller banks that the position for the individual responsible for IT was vacant and would be filled only later during 2012. Therefore, the number of possible respondents for questionnaire B was set at 15. The overall questionnaire response rate achieved for this study was 84%, which is deemed very high. Effectively, an overall response rate of 90% was achieved (including null responses). A questionnaire response rate of 94% was achieved for the company secretaries. A questionnaire response rate of 73% was achieved for the individuals responsible for IT. The effective response rate for the individuals responsible for IT was 87% (including null responses). The unique nature of this study and the lack of empirical research on the topics discussed in this thesis from the South African banking sector perspective ensure insightful results regardless of the response rate. The disclosure of IT governance practices and the controversial nature of hacking and ethical hacking might have made some of the individuals responsible for IT reluctant to participate, although only one specifically highlighted this. One individual responsible for IT indicated that he could not participate in the survey due to the bank’s internal policy not to participate in research questionnaires.

### 8.12 CHAPTER SUMMARY

This chapter outlined the research methodology followed in this thesis with particular reference to the two questionnaires applied in a mixed-method approach. Self-administered questionnaires were sent to the company secretaries and individuals responsible for IT at each of the locally registered banks. The results of the questionnaires are presented in Chapter 9.
CHAPTER 9
Research findings and recommendations

9.1 INTRODUCTION

This chapter presents the results of the empirical fieldwork that was conducted in the banking sector in South Africa by way of the questionnaires discussed in Chapter 8. The questionnaire design was based on the thematological questions that were defined throughout the literature study. The research findings are based on the outcome of the questionnaires sent to the company secretary and the individuals responsible for IT at each of the locally registered banks in South Africa. Comparisons are also drawn with the analysis of similar questions between the company secretaries, individuals responsible for IT and annual reports. The recommendations are based on the results of the questionnaires and the analysis comparisons, while areas for further research will be outlined in Chapter 10.

9.2 RESEARCH FINDINGS OF THE COMPANY SECRETARY QUESTIONNAIRE

The results from the questionnaires completed by the company secretaries are analysed below and provide a view on the IT governance, IT risk management and ethical hacking practices at locally registered banks. The company secretary questionnaire (Questionnaire A) is included in Annexure A of this thesis and the questions contained therein will be analysed in the paragraphs below.

9.2.1 Company secretaries’ corporate governance role

9.2.1.1 Objective of the question

The objective with this set of questions was to determine the level of support the company secretaries receive in carrying out their corporate governance responsibilities (Question 1).

9.2.1.2 Findings and deductions

Section 8.5.1 highlighted that the board of directors needs to support the role of the company secretary. The findings below indicate that almost all company secretaries (93%)
felt that they received enough support from the board of directors to perform their corporate governance responsibilities.

Table 9.1  The company secretaries’ corporate governance role (own calculation from company secretary questionnaire) (n = 15)

<table>
<thead>
<tr>
<th>Company secretaries’ corporate governance role</th>
<th>Yes</th>
<th>%</th>
<th>No</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you get enough support from the board of directors to perform your corporate governance responsibilities?</td>
<td>14</td>
<td>93%</td>
<td>1</td>
<td>7%</td>
</tr>
<tr>
<td>Do you have the freedom to add new corporate governance issues to the agenda of the board?</td>
<td>13</td>
<td>87%</td>
<td>2</td>
<td>13%</td>
</tr>
<tr>
<td>Do you believe that enough guidance is provided by professional and regulatory bodies in terms of your corporate governance responsibilities?</td>
<td>12</td>
<td>80%</td>
<td>3</td>
<td>20%</td>
</tr>
</tbody>
</table>

It has been established in section 8.5.1 that the company secretary plays a key role in setting the agenda of topics to be covered by the board of directors. The results in Table 9.1 indicate that most company secretaries (87%) were allowed to add new corporate governance issues to the agenda of the board of directors. One of the company secretaries, who answered no to the support question, commented as follows:

- “The issues will only be added after consultation with the chairman”.

Two company secretaries have therefore indicated that they are restricted from adding pertinent issues to the agenda of the board.

Overall, what can be deduced from these responses is that if the company secretary had a particular concern regarding IT risk or hacking, he or she would be in a position to bring that to the attention of the board of directors. However, a comment from one of the company secretaries alludes to the fact that at least in one bank, IT matters are referred to a supporting sub-committee of the board:

- “A dedicated sub-committee of the Board is in place to ensure that the IT function is adequately governed.”

At least 80% of company secretaries felt that enough guidance is provided by professional and regulatory bodies in terms of their corporate governance responsibilities. As highlighted in section 8.5.1, professional bodies such as the ICSA play a role here in providing adequate guidance.
9.2.2 The company secretaries’ views on the board and IT governance

9.2.2.1 Objective of the question

The purpose of the set of statements included in the second question in the questionnaire was to determine whether, from the company secretaries’ perspective, the board of directors focuses enough on IT matters, which includes aspects such as IT governance, IT risk, cybercrime and hacking (Question 2).

9.2.2.2 Findings and deductions

The following Likert scale was used by participants to rank the statements presented in Table 9.2: 1 = Agree completely; 2 = Agree to a large extent; 3 = Agree to a moderate extent; 4 = Agree to a lesser extent; 5 = Don’t agree at all.

<table>
<thead>
<tr>
<th>The board and IT governance</th>
<th>Agree completely</th>
<th>Agree to a large extent</th>
<th>Agree to a moderate extent</th>
<th>Agree to a lesser extent</th>
<th>Don’t agree at all</th>
<th>n</th>
<th>Weighted arithmetic mean</th>
<th>Mean</th>
<th>Standard deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>The board of directors takes responsibility for IT governance.</td>
<td>9</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>15</td>
<td>4.40</td>
<td>1.60</td>
<td>0.83</td>
</tr>
<tr>
<td>The board of directors effectively address IT governance.</td>
<td>8</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>15</td>
<td>4.20</td>
<td>1.80</td>
<td>1.08</td>
</tr>
<tr>
<td>The board members have the necessary skills to deal with IT matters.</td>
<td>1</td>
<td>5</td>
<td>5</td>
<td>3</td>
<td>1</td>
<td>15</td>
<td>3.13</td>
<td>2.87</td>
<td>1.06</td>
</tr>
<tr>
<td>IT governance is a key component of corporate governance in our organisation.</td>
<td>7</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>0</td>
<td>15</td>
<td>4.00</td>
<td>2.00</td>
<td>1.13</td>
</tr>
<tr>
<td>IT governance is high on the board’s agenda.</td>
<td>8</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>15</td>
<td>4.00</td>
<td>2.00</td>
<td>1.20</td>
</tr>
<tr>
<td>Our IT governance practices compare favourably with those of our competitors.</td>
<td>5</td>
<td>7</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>14</td>
<td>4.14</td>
<td>1.86</td>
<td>0.86</td>
</tr>
<tr>
<td>The board’s overall response to IT risk is good.</td>
<td>9</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>15</td>
<td>4.47</td>
<td>1.53</td>
<td>0.74</td>
</tr>
<tr>
<td>The board’s overall response to cybercrime is good.</td>
<td>8</td>
<td>5</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>15</td>
<td>4.27</td>
<td>1.73</td>
<td>1.10</td>
</tr>
<tr>
<td>The board’s overall response to hacking is good.</td>
<td>8</td>
<td>5</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>15</td>
<td>4.27</td>
<td>1.73</td>
<td>1.10</td>
</tr>
</tbody>
</table>

*One respondent did not choose an option

The majority of company secretaries (60% agreed completely and 20% agreed to a large extent) were of the opinion that the board of directors deals appropriately with IT governance as part of its corporate governance responsibilities. In contrast, however, more than half of the company secretaries agreed to a moderate extent (33%) or less (27%) that the board of directors does not necessarily have enough IT skill to deal with IT matters effectively. This
was highlighted, despite the company secretary’s responsibility to ensure that the board of directors receives appropriate training, as discussed in section 8.5.1. Responses were in fact varied regarding IT skill, as reflected in the lowest weighted arithmetic mean and highest mean in Table 9.2. The comments from the company secretaries indicate that IT governance responsibilities are delegated to other parties in the organisation:

- “Accountability for IT governance is vested with the Risk Committee on behalf of the board – this committee has the necessary skills.”
- “While the board members are not IT experts, they do have qualified people in the IT department. They also rely on internal & external audit reports.”
- “IT governance is the responsibility of the bank’s Risk and Capital Management Committee, which reports to the board.”
- “The board effectiveness is a function of the trust put in management.”

As highlighted in section 8.5.1, the company secretary plays a key role in ensuring that the board of directors adheres to the latest principles of good corporate governance, which includes IT governance. Most banks (94%) have disclosed in their annual reports that they follow principles of good corporate governance (Table 7.2), although only 56% disclosed their IT governance practices (Table 7.3). The majority of company secretaries were confident (33% agreed completely and 47% agreed to a large extent) that their IT governance practices compare favourably with other banks. In terms of the responses to IT risk, cybercrime and hacking, the company secretaries were slightly more at ease with the board of directors’ focus on IT risk in general (60% agreed completely and 27% agreed to a large extent, reflected in the lowest standard deviation of 0.74 in Table 9.2). Slightly less confidence was displayed in the overall response to cybercrime and hacking, both considered IT risks. As part of the company secretaries’ responsibilities good risk management practices should be followed in the organisation (as highlighted in section 8.5.1) and more focus should be placed on these IT risks.

### 9.2.3 The company secretaries’ views on IT in business

#### 9.2.3.1 Objective of the question

The third question in the questionnaire comprised statements that were aimed at assessing, from the company secretaries’ perspective, the significance of IT in their respective banks and also each bank’s general ability to deal with IT risk and cybercrime (Question 3).
9.2.3.2 Findings and deductions

The following Likert scale was used by participants to rate the statements in Table 9.3: 1 = Agree completely; 2 = Agree to a large extent; 3 = Agree to a moderate extent; 4 = Agree to a lesser extent; 5 = Don’t agree at all.

Table 9.3 The company secretaries’ general views on IT in business (own calculation from company secretary questionnaires) (n = 15)

<table>
<thead>
<tr>
<th>General views on IT in business</th>
<th>Agree completely</th>
<th>Agree to a large extent</th>
<th>Agree to a moderate extent</th>
<th>Agree to a lesser extent</th>
<th>Don’t agree at all</th>
<th>Weighted arithmetic mean</th>
<th>Mean</th>
<th>Standard deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our ability to deal with IT challenges is good.</td>
<td>6</td>
<td>6</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>4.13</td>
<td>1.87</td>
<td>0.92</td>
</tr>
<tr>
<td>Our ability to deal with IT risk is good.</td>
<td>5</td>
<td>7</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>4.13</td>
<td>1.87</td>
<td>0.74</td>
</tr>
<tr>
<td>IT plays a key enabling role in our products and services.</td>
<td>10</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4.67</td>
<td>1.33</td>
<td>0.49</td>
</tr>
<tr>
<td>Our IT governance practices are key to fighting cybercrime.</td>
<td>7</td>
<td>6</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>4.27</td>
<td>1.73</td>
<td>0.88</td>
</tr>
</tbody>
</table>

Almost all of the company secretaries (67% agreed completely and 33% agreed to a large extent) agreed that IT plays a key enabling role in their organisation (also reflected in the low standard deviation value of 0.49 in Table 9.3). Company secretaries play a role in advising the board of directors on risk management practices (as established in section 8.5.1). The banks’ ability to deal with IT challenges or IT risk was considered as satisfactory overall (40% agreed completely and 40% agreed to a large extent). Nonetheless, 20% of respondents agreed only to a moderate extent that IT risk is dealt with adequately.

At least three banks are at risk of not effectively mitigating their IT risks, according to their company secretaries. Also, most company secretaries were confident that the organisation’s IT governance was either fully (47%) or to a large extent (40%) effective in addressing cybercrime. Despite this, three respondents (20%) were not so confident that their organisations deal effectively with IT challenges, and two respondents (13%) indicated that their IT governance practices were not key in fighting cybercrime. Therefore, there is scope for the company secretaries to play a stronger role in ensuring that IT governance practices are a focal point for the board of directors.
9.2.4 The company secretaries’ views on incorporating IT governance into the organisation

9.2.4.1 Objective of the question

The purpose of the fourth question was to determine what the key driving factors are behind incorporating IT governance practices in the organisations (Question 4), therefore providing some insight into whether IT governance is seen as essential to the organisation, or compulsory in nature, by way of ranking specific factors.

9.2.4.2 Findings and deductions

In Question 4, respondents were asked to rank five key drivers towards incorporating IT governance into their organisations. One respondent incorrectly applied the ranking in this question, by ranking more than one option in first position. The results were used as is and are depicted in the graph presented in Figure 9.1. The results presented in Table 9.4 are sorted in descending order according to the rankings.

<table>
<thead>
<tr>
<th>Incorporating IT governance into the organisation</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
<th>4th</th>
<th>5th</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulatory requirements or legislation.</td>
<td>8</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Achieving business objectives or strategy.</td>
<td>6</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Growth in complexity of the IT function.</td>
<td>2</td>
<td>6</td>
<td>4</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Industry norm and practice.</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>The culture of the organisation.</td>
<td>0</td>
<td>3</td>
<td>4</td>
<td>2</td>
<td>6</td>
</tr>
</tbody>
</table>

The results indicate that company secretaries were of the opinion the regulatory requirements or legislation is the key driving factor behind incorporating IT governance practices in the organisation (53% of respondents ranked it in first position). This could be due to the inclusion of IT governance principles in King III. After all, it is the company secretary’s responsibility to ensure that corporate governance practices are followed (as established in section 8.5.1). IT governance might therefore be seen as compulsory, rather than essential. Achieving business objectives or strategy has been ranked second, which is in contrast with the first key driver and indicates that at least some company secretaries (40% ranked it in first position) believe IT governance is an important driver towards achieving business objectives.
Growth in complexity of the IT function was ranked in third position, which indicates that IT governance is essential for a growing bank. More than half of the company secretaries did not believe that industry norm and practice is a driving factor (33% ranked in fourth and 27% in fifth position). This is also an indication that industry frameworks do not play a vital role in informing IT governance practices. IT governance practices might therefore be immature in the South African banking sector. According to the company secretaries, the culture of the organisation does not play a key role in influencing IT governance practices (40% ranked it in fifth position), which implies that the need for IT governance is not ingrained yet in the culture of some of the banks.

9.2.5 The company secretaries’ views on the individual responsible for IT

9.2.5.1 Objective of the question

The objective behind the fifth set of questions was to determine whether the company secretary is of the opinion that the individual responsible for IT is sufficiently qualified and experienced to fulfil this particular role. In addition, the reporting line of the individual responsible for IT was determined, which is also an indication of the significance attributed to IT in the organisation (Question 5). A combination of yes/no questions and specific questions and rankings were applied in achieving this objective.
### 9.2.5.2 Findings and deductions

**Table 9.5** The company secretaries’ views on the individuals responsible for IT (own calculation from company secretary questionnaires)

<table>
<thead>
<tr>
<th>The individual responsible for IT</th>
<th>n</th>
<th>Yes</th>
<th>%</th>
<th>No</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Has your organisation appointed an individual responsible for the management of IT?</td>
<td>15</td>
<td>15</td>
<td>100%</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Do you think the individual responsible for IT is suitably qualified to deal with IT governance?</td>
<td>15</td>
<td>14</td>
<td>93%</td>
<td>1</td>
<td>7%</td>
</tr>
<tr>
<td>Do you think the individual responsible for IT is suitably experienced to deal with IT governance?</td>
<td>14*</td>
<td>13</td>
<td>93%</td>
<td>1</td>
<td>7%</td>
</tr>
<tr>
<td>Is the individual responsible for IT invited to attend board of directors meetings?</td>
<td>15</td>
<td>9</td>
<td>60%</td>
<td>6</td>
<td>40%</td>
</tr>
<tr>
<td>Has the overall responsibility for IT been assigned to a particular board member?</td>
<td>15</td>
<td>5</td>
<td>33%</td>
<td>10</td>
<td>67%</td>
</tr>
</tbody>
</table>

*One respondent did not answer the question

All the organisations who participated have an individual appointed to oversee the IT function. Almost all of the company secretaries (93%) were of the opinion that this individual was appropriately qualified and experienced for this role. The majority of the individuals responsible for IT are invited to attend the board of directors’ meetings (60%). This is low considering the significance of IT as a business enabler. Two company secretaries provided the following comments, regarding attendance of committees:

- “The CIO: Only by invitation but attends audit committee.”
- “At each risk committee / to the risk committee.”

Only 33% of the banks have allocated the responsibility for IT to a particular board member. Either this is an indication that IT does not feature prominently enough at the board of directors level or the question could have been interpreted to say that IT responsibility should be allocated to all board members and not to one member exclusively. In case of the former interpretation, it implies that the banking sector does not fully comply with the requirements of King III, which places the responsibility of IT governance with the board of directors (IoD, 2009b:82). Given the corporate governance role of the board of directors and its responsibility in identifying IT risks as part of its risk management oversight responsibilities (discussed in section 5.3.1), it is questionable whether the board of directors fully fulfils these duties in the South African banking sector. It is also questionable whether the company secretaries fulfilled their corporate governance duties, by adequately informing the board of directors about corporate governance best practice (as discussed in section 8.5.1).
Table 9.6  Job title of the individual responsible for IT (own calculation from company secretary questionnaires)

<table>
<thead>
<tr>
<th>Job title</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chief Information Officer (CIO).</td>
<td>9</td>
</tr>
<tr>
<td>Chief Technology Officer (CTO).</td>
<td>0</td>
</tr>
<tr>
<td>Executive: IT.</td>
<td>1</td>
</tr>
<tr>
<td>Head of IT.</td>
<td>3</td>
</tr>
<tr>
<td>Other (Chief Manager IT; Manager: IT).</td>
<td>2</td>
</tr>
</tbody>
</table>

As already established, banks do not generally disclose details of their appointed CIOs (effectively, only two banks disclosed this in their annual reports as reflected in Table 7.5). The questionnaire results indicate that the title CIO is used by nine of the banks (60%), which is an indication of a relatively senior position in the organisation, but also highlights the importance of the IT function in the banking sector. Other smaller banks, such as Mercantile Bank Limited, African Bank Limited, Albaraka Bank Limited, HBZ Bank Limited, the South African Bank of Athens and Habib Overseas Bank used titles, such as head of IT or IT manager, which indicates that their IT operations are smaller than those of other banks.

Table 9.7  Reporting line of the individual responsible for IT (own calculation from company secretary questionnaires)

<table>
<thead>
<tr>
<th>Reporting line</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chief Operating Officer (COO).</td>
<td>5</td>
</tr>
<tr>
<td>Chief Financial Officer (CFO).</td>
<td>1</td>
</tr>
<tr>
<td>Chief Executive Officer (CEO).</td>
<td>6</td>
</tr>
<tr>
<td>Board of directors</td>
<td>1</td>
</tr>
<tr>
<td>Audit committee.</td>
<td>0</td>
</tr>
<tr>
<td>Other (Executive: Operations; Financial Director).</td>
<td>2</td>
</tr>
</tbody>
</table>

Many of the individuals responsible for IT report to the CEO (40%), which is an indication of the individual responsible for IT holding a senior position in the organisation. Some respondents report to the COO (33%), which is a possible indication that the COO may take ultimate responsibility for IT in the organisation. However, this is not always the case, where the CIO might have a more senior role in the organisation, as reflected in the following comment from one of the company secretaries:

- “Although the CIO reports to the COO, he is also a full member of Exco.”

It also appears that the CIOs are not board of director members, seeing that they are typically positioned at executive management level in the organisation. Another comment from one of the smaller banks indicates that individuals responsible for IT at smaller banks do not necessarily represent IT at a senior level: “The person responsible for IT reports directly to the financial director, who sits at all board meetings and answers questions pertaining to IT”. This is a further indication that IT and IT governance may not feature
prominently enough at the board of directors level.

The following Likert scale was used by participants to rank the statements presented in Table 9.8: 1 = Agree completely; 2 = Agree to a large extent; 3 = Agree to a moderate extent; 4 = Agree to a lesser extent; 5 = Don’t agree at all.

Table 9.8  The company secretaries’ views on the individual responsible for IT achieving business objectives (own calculation from company secretary questionnaires) (n = 15)

<table>
<thead>
<tr>
<th>The individual responsible for IT meeting business objectives</th>
<th>Agree completely</th>
<th>Agree to a large extent</th>
<th>Agree to a moderate extent</th>
<th>Agree to a lesser extent</th>
<th>Don’t agree at all</th>
<th>Weighted arithmetic mean</th>
<th>Mean</th>
<th>Standard deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>The individual responsible for IT understands how to integrate IT governance into the business.</td>
<td>5</td>
<td>6</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>4.07</td>
<td>1.93</td>
<td>0.80</td>
</tr>
<tr>
<td>The individual responsible for IT ensures that IT solutions meet the strategic objectives of the organisation.</td>
<td>7</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4.47</td>
<td>1.53</td>
<td>0.52</td>
</tr>
</tbody>
</table>

As highlighted in section 5.6.1, the role of the CIO is paramount in establishing IT governance in the organisation. Most company secretaries agree that the individual responsible for IT integrates IT governance into the business (33% agreed completely and 40% agreed to a large extent). Most company secretaries were also of the opinion that the individual responsible for IT ensures that the IT solutions meet the strategic objectives of the bank (47% agreed completely and 53% agreed to a large extent, also reflected in the lower standard deviation value of 0.52). But it must be noted that four respondents only agreed to a moderate extent that the individual responsible for IT understands how to integrate IT into business.

The following comment from one of the company secretaries sheds some light on the role of the individual responsible for IT:

• “His role is that of ensuring, smooth operation of the business through IT, not governance. However, with internal & external audit, as well as the compliance department, he fulfils his governance function for IT.”

Therefore, the individual responsible for IT might have more of an operational function at some banks, rather than a governance role. The governance role could be fulfilled to some extent by other functions or committees in the organisation. This is evident from another comment by a company secretary:
“IT governance is overseen by the Risk and Capital Management Committee, which committee is composed of non-executive directors.”

9.2.6 The company secretaries’ views on committees dealing with IT

9.2.6.1 Objective of the question

The purpose of the two aspects included in question 7 was to identify which board and non-board committees’ deals with IT matters (Question 7).

9.2.6.2 Findings and deductions

In Table 9.9, similar board committees were grouped together and one count was awarded for each type of committee. One respondent did not answer this question.

Almost all banks have disclosed that they do have a risk management committee (Table 7.2). In most banks, the board level risk committees deal with IT matters. A risk committee will focus mostly on IT risk or technology risk encountered in the organisation, as opposed to other non-risk-related IT matters.

<table>
<thead>
<tr>
<th>Board committees</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk and Capital Management Committee / Risk Management Committee / Risk Committee.</td>
<td>10</td>
</tr>
<tr>
<td>IT Committee / Technology Committee.</td>
<td>3</td>
</tr>
<tr>
<td>Board of directors.</td>
<td>1</td>
</tr>
<tr>
<td>Other (Audit Committee).</td>
<td>1</td>
</tr>
</tbody>
</table>

Therefore, sufficient coverage of IT matters may not be achieved when IT matters are delegated to the risk management committee only. Three banks indicated that they have an IT or technology committee, positioned as board committees. Only one respondent indicated that IT matters are dealt with at the board of directors’ meetings (although the question could be interpreted as “board committees, other than the board of directors itself”). Only one company secretary indicated that IT matters are dealt with at an audit committee level, despite the recommendation set by King III that audit committees should ensure IT risk has been dealt with from a financial reporting perspective (discussed in section 4.3.5.5). Nonetheless, most banks delegate their IT matters to other board committees. This indicates that IT governance has not been fully positioned at the board of directors level yet by most
banks and may not carry the same weight as other corporate governance or business issues. This is also in contrast with the requirements of King III, which requires the IT steering committee to be positioned at a board committee level (IoD, 2009b:46) and not a management committee level.

Turning now to non-board committees, in Table 9.10, similar board committees were grouped together and one count was awarded for each type of committee (some participants listed several committees of the same type). One respondent did not answer this question.

Table 9.10 The company secretaries’ views on non-board committees dealing with IT matters (own calculation from company secretary questionnaires) (n = 14)

<table>
<thead>
<tr>
<th>Non-board committees</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Committee / Risk and Capital Management Committee / Operational Risk Committee / Enterprise Risk Committee / Technology Enterprise Risk Committee / IT Risk Committee.</td>
<td>5</td>
</tr>
<tr>
<td>IT Committee / Technology Committee / IT Steering Committee / Executive IT Committee / Technology Operational Meeting / Technology Exco / IT Forum / IT Manco.</td>
<td>9</td>
</tr>
<tr>
<td>Group Executive Committee / Executive Management Committee / Exco.</td>
<td>5</td>
</tr>
<tr>
<td>Other (Group Operational Meeting; Financial Review Forum; Business Engagement Reviews; Business Acceptance Committee; Compliance Committee; Prioritisation Forum; Group Strategic Technology &amp; Operations Forum).</td>
<td>4</td>
</tr>
</tbody>
</table>

The results in Table 9.10 above support the findings of the previous question, in that IT matters are mostly dealt with at non-board level, as opposed to board level committees. Most banks (9 out of 16) have some kind of IT executive management committee, such as an IT steering committee. This result is in line with the number of banks which disclosed that they have an IT steering committee (Table 7.3). IT matters are also discussed at risk management committees, as well as several other management committees. King III states that the board of directors is allowed to delegate responsibilities to other committees, without relinquishing their own responsibilities (IoD, 2009b:49). Seeing that IT issues are mostly dealt with at non-board committees, it does appear to some extent that the board of directors in the banking sector are not fulfilling their IT responsibilities. Furthermore, it is also unlikely that IT risks, such as hacking, will be discussed in depth at the board of directors level. The company secretaries can play a stronger role in ensuring that corporate best practices are being followed (which is part of their responsibilities, as established in section 8.5.1) and that more attention is paid at board level to issues such as hacking and cybercrime.
It is the company secretary’s responsibility to assist the chairman of the board in setting the agenda and also facilitating the flow of information between management and the board of directors (as discussed in section 8.5.1). The majority of the company secretaries (73%) indicated that the board of directors has insight into the briefing notes or minutes of IT matters discussed at other committees. At least this implies that information pertaining to IT issues and risks discussed and disclosed at other committees (such as IT steering committees) is made available to the board of directors. However, the company secretaries at four banks either did not have the opportunity to disclose IT matters or might not have included the IT matters in the board of directors’ meeting minutes. Therefore, not all banks have full insight into IT matters at their organisation. Almost all the company secretaries included IT governance as a board of directors’ agenda point. This is not surprising, seeing that King III places the responsibility for IT governance with the board of directors. The degree of detail covered in IT governance discussions or submissions in the form of meeting minutes at the board of directors level is however unknown. What is known is that IT governance is not disclosed by all banks and only five banks provided an extensive discussion of IT governance in their annual reports (Table 7.3). Some organisations prefer to delegate their IT matters to other committees, as is evident from the following quotes:

- “IT matters are included in the agenda of the Risk and Capital Management Committee, and the deliberations of such committee are reported to the board by the chairman of that committee.”
- “As part of a Group of companies, our IT matters are discussed at Group level (Holding company IT governance structures).”

Almost all of the company secretaries (93%) have indicated that IT matters are routinely included in the board of directors’ agenda. This is an indication that IT matters have grown in

<table>
<thead>
<tr>
<th>Frequency of IT matters included in board’s agenda</th>
<th>Count</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Never.</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Case by case.</td>
<td>1</td>
<td>7%</td>
</tr>
<tr>
<td>Routinely.</td>
<td>14</td>
<td>93%</td>
</tr>
<tr>
<td>Do not know.</td>
<td>0</td>
<td>0%</td>
</tr>
</tbody>
</table>
importance and are brought to the attention of the board of directors. Nonetheless, it still needs to be considered that meeting minutes prepared for the board of directors may not include a detailed submission of IT matters, at least at some banks. This is a concern, since the board of directors may not have all the relevant information pertaining to IT matters available to it, to allow it to make an informed decision.

9.2.7 The company secretaries’ views on business risk and IT risk

9.2.7.1 Objective of the question

The purpose of the eighth question was to determine the level of awareness of how IT risk is linked with business risks in the organisation (Question 8).

9.2.7.2 Findings and deductions

The following Likert scale was used by participants to rank the statements presented in Table 9.13: 1 = To a large extent; 2 = To a moderate extent; 3 = To a small extent; 4 = Not at all. The results in Table 9.13 were sorted in descending order according to the weighted arithmetic mean.

<table>
<thead>
<tr>
<th>IT risk linked to business risk</th>
<th>To a large extent</th>
<th>To a moderate extent</th>
<th>To a small extent</th>
<th>Not at all</th>
<th>Weighted arithmetic mean</th>
<th>Mean</th>
<th>Standard deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology risk.</td>
<td>13</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>3.73</td>
<td>1.27</td>
<td>0.80</td>
</tr>
<tr>
<td>Business continuity risk.</td>
<td>12</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>3.60</td>
<td>1.40</td>
<td>0.91</td>
</tr>
<tr>
<td>Disaster recovery risk.</td>
<td>12</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>3.60</td>
<td>1.40</td>
<td>0.91</td>
</tr>
<tr>
<td>Operational risk.</td>
<td>10</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>3.53</td>
<td>1.47</td>
<td>0.83</td>
</tr>
<tr>
<td>Reputational risk.</td>
<td>9</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>3.27</td>
<td>1.73</td>
<td>1.03</td>
</tr>
<tr>
<td>Compliance risk.</td>
<td>6</td>
<td>5</td>
<td>3</td>
<td>1</td>
<td>3.07</td>
<td>1.93</td>
<td>0.96</td>
</tr>
<tr>
<td>Credit risk.</td>
<td>6</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>3.07</td>
<td>1.93</td>
<td>0.88</td>
</tr>
<tr>
<td>Market risk.</td>
<td>7</td>
<td>2</td>
<td>5</td>
<td>1</td>
<td>3.00</td>
<td>2.00</td>
<td>1.07</td>
</tr>
<tr>
<td>Human resource risk.</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>1</td>
<td>2.93</td>
<td>2.07</td>
<td>0.96</td>
</tr>
<tr>
<td>Physical risk.</td>
<td>2</td>
<td>6</td>
<td>5</td>
<td>2</td>
<td>2.53</td>
<td>2.47</td>
<td>0.92</td>
</tr>
</tbody>
</table>

Considering that Chapter 4 has presented the case of close links between business risk and IT risk, how this is perceived in the banking sector is important. For example, the SARB requires banks to manage and mitigate various business risks (section 4.2.3). Company secretaries are also required to have a thorough understanding of risk management, as well
as the type of risks that may affect the organisation (highlighted in section 8.5.1). The questionnaire results indicated that technology risk has been ranked as the risk largely affected by IT risk (87% agreed to a large extent, with the standard deviation of 0.80 clearly the lowest in the table), followed by business continuity and disaster recovery, which were ranked equally (80% agreed to a large extent).

Despite the apparent importance of technology risk, this has not been disclosed as a significant risk in the annual reports (only 31% disclosed technology risk, as indicated in Table 7.6). The first three risks in Table 9.13 are clearly easily associated with IT risk, although not exclusively related to IT per se. Operational risk has been disclosed by all the banks in their annual reports (Table 7.6). Operational risk has been ranked in fourth position in the table above, as a clear indication that IT keeps the bank operational and IT risk would be a threat. Most company secretaries do realise that reputational risk can be affected by IT risk. The company secretaries have indicated that compliance risk, credit risk and market risk are only affected by IT risk at some banks. What is concerning is that the link between physical risk and IT risk is not well understood (highlighted by the low weighted arithmetic mean of 2.53). Physical risk has also only been disclosed in 25% of the annual reports (Table 7.6). Banks in general tend to have strict physical security mechanisms in place and this may be reason why this is not seen as a particular area of concern. Perhaps company secretaries do not understand the reality of social engineering and the likelihood of hackers physically entering a bank’s premises (discussed in sections 3.6 and 3.8.3). Similarly, human resource risk and the link with IT risk are not well understood. Human resource risk has also only been disclosed in 38% of the annual reports (Table 7.6). Human resource risk can be linked to attacks by insiders (such as disgruntled employees, as discussed in section 3.5.3.6). This is not understood by company secretaries and indicates that company secretaries might not be fully fulfilling their risk management responsibilities. The low scores for human resource risk and physical risk are an indication that some banks in the local banking sector might be at risk of being attacked by insiders or hackers using social engineering techniques.

9.2.8 The company secretaries' views on hacking and IT risk

9.2.8.1 Objective of the question

The objective behind the ninth question was to determine whether the company secretaries understand the link between hacking and a number of IT risk themes (Question 9).
9.2.8.2 Findings and deductions

The following Likert scale was used by participants to rank the statements presented in Table 9.14: 1 = To a large extent; 2 = To a moderate extent; 3 = To a small extent; 4 = Not at all. The results in Table 9.14 were sorted in descending order according to the weighted arithmetic mean.

Table 9.14  The company secretaries’ views on hacking increasing various IT risks (own calculation from company secretary questionnaire) (n = 15)

<table>
<thead>
<tr>
<th>Hacking increasing the IT risks below</th>
<th>To a large extent</th>
<th>To a moderate extent</th>
<th>To a small extent</th>
<th>Not at all</th>
<th>Weighted arithmetic mean</th>
<th>Mean</th>
<th>Standard deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybercrime.</td>
<td>12</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3.80</td>
<td>1.20</td>
<td>0.41</td>
</tr>
<tr>
<td>Logical access risk.</td>
<td>11</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>3.67</td>
<td>1.33</td>
<td>0.62</td>
</tr>
<tr>
<td>IT systems risk.</td>
<td>10</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>3.60</td>
<td>1.40</td>
<td>0.63</td>
</tr>
<tr>
<td>IT continuity risk.</td>
<td>10</td>
<td>3</td>
<td>2</td>
<td>0</td>
<td>3.53</td>
<td>1.47</td>
<td>0.74</td>
</tr>
<tr>
<td>Communications failure.</td>
<td>8</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>3.47</td>
<td>1.53</td>
<td>0.64</td>
</tr>
<tr>
<td>IT non-compliance risk.</td>
<td>9</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>3.27</td>
<td>1.73</td>
<td>1.03</td>
</tr>
<tr>
<td>Physical access risk.</td>
<td>6</td>
<td>6</td>
<td>3</td>
<td>0</td>
<td>3.20</td>
<td>1.80</td>
<td>0.77</td>
</tr>
<tr>
<td>IT human resources risk.</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>1</td>
<td>2.80</td>
<td>2.20</td>
<td>0.94</td>
</tr>
<tr>
<td>Lack of software development.</td>
<td>2</td>
<td>7</td>
<td>3</td>
<td>3</td>
<td>2.53</td>
<td>2.47</td>
<td>0.99</td>
</tr>
</tbody>
</table>

Company secretaries are required to be familiar with pertinent risks that may affect the industry (discussed in section 8.5.1). It follows, then, that as IT risk is a significant risk in the banking sector, company secretaries should have a good understanding of IT risk. Again, as argued in Chapter 4, there is a strong link between the various IT risk themes (which have been summarised in this question) and hacking. The link between cybercrime and hacking was well understood by almost all (80%) the company secretaries (also supported by the lowest standard deviation value). One respondent specifically highlighted this reality in the following quote: “Banks remain a target for cybercrime and attacks from external as well as internal.” The link between logical access risks, IT systems risk, IT continuity risk and hacking were also well understood. Software or project management practices have been disclosed in only 25% of the annual reports (Table 7.7), which is an indication of the relative low importance of software development practices. The company secretaries did not comprehend how the lack of software development could be affected by hacking (discussed in section 3.8.5) and no further comments were provided to clarify the responses. Weak software development practices, neglecting security controls, may lead to exploitable vulnerabilities.

The varied responses by the company secretaries indicates that the company secretaries
did not understand how *IT human resource risk* could be increased by hacking and had not considered, for example, the possibility of disgruntled IT employees conducting insider hacker attacks (as highlighted in section 3.5.3.6). The findings indicate that company secretaries are familiar with only some (mostly obvious) IT risks and do not fully understand how IT risks, such as *IT human resource risk* and *lack of software development practices* (varied responses according to the high standard deviation scores of 0.94 and 0.99) could lead to hacker attacks.

9.2.9 The company secretaries' views on general responses to hacking

9.2.9.1 Objective of the question

The purpose of the tenth question was to focus on the responses to hacking identified in this thesis, in order to identify if those are used within the participant's bank, and, secondly, to test the effectiveness thereof (Question 10).

9.2.9.2 Findings and deductions

The following Likert scale was used by participants to rank the statements presented in Table 9.15 and Table 9.16: 1 = Agree completely; 2 = Agree to a large extent; 3 = Agree to a moderate extent; 4 = Agree to a lesser extent; 5 = Don't agree at all. The results in Tables 9.15 and 9.16 were sorted in descending order according to the weighted arithmetic mean.

Table 9.15 The company secretaries’ views on the extent of general responses to the risk of hacking (own calculation from company secretary questionnaires)

<table>
<thead>
<tr>
<th>The extent of general responses to hacking</th>
<th>Agree completely</th>
<th>Agree to a large extent</th>
<th>Agree to a moderate extent</th>
<th>Agree to a lesser extent</th>
<th>Don’t agree at all</th>
<th>n</th>
<th>Weighted arithmetic mean</th>
<th>Mean</th>
<th>Standard deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security technologies, such as firewalls.</td>
<td>10</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>15</td>
<td>4.40</td>
<td>1.60</td>
<td>1.12</td>
</tr>
<tr>
<td>Information security management.</td>
<td>7</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>15</td>
<td>4.29</td>
<td>1.71</td>
<td>1.07</td>
</tr>
<tr>
<td>Internal control.</td>
<td>8</td>
<td>5</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>15</td>
<td>4.27</td>
<td>1.73</td>
<td>1.10</td>
</tr>
<tr>
<td>IT governance.</td>
<td>8</td>
<td>5</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>15</td>
<td>4.27</td>
<td>1.73</td>
<td>1.10</td>
</tr>
<tr>
<td>Risk management.</td>
<td>6</td>
<td>7</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>15</td>
<td>4.13</td>
<td>1.87</td>
<td>1.06</td>
</tr>
<tr>
<td>Software development practices.</td>
<td>6</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>15</td>
<td>3.93</td>
<td>2.07</td>
<td>1.22</td>
</tr>
<tr>
<td>Corporate governance.</td>
<td>4</td>
<td>6</td>
<td>2</td>
<td>1</td>
<td>4</td>
<td>15</td>
<td>3.60</td>
<td>2.40</td>
<td>1.35</td>
</tr>
<tr>
<td>Ethical hacking.</td>
<td>5</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>15</td>
<td>3.40</td>
<td>2.60</td>
<td>1.68</td>
</tr>
<tr>
<td>Governance frameworks, such as CobiIT.</td>
<td>2</td>
<td>7</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>15</td>
<td>3.40</td>
<td>2.60</td>
<td>1.24</td>
</tr>
<tr>
<td>Applying service and quality management, such as ITIL.</td>
<td>3</td>
<td>6</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>15</td>
<td>3.20</td>
<td>2.80</td>
<td>1.57</td>
</tr>
</tbody>
</table>

*One respondent did not answer this question
Company secretaries are required to be familiar with general responses to IT risk, such as risk management and internal control (established in section 8.5.1). Security technologies such as firewalls have been rated as the most common response to hacking attacks (supported by the highest weighted arithmetic mean of 4.40 and a mean value of 1.60). Indeed, these will be deployed by most, if not all, banks as a response to hacking attacks. Yet, as this study has argued, organisations are over-reliant on security technologies, which do not always provide adequate protection against hacker attacks (discussed in section 5.9.9). The banking sector therefore might be under the impression that it is adequately protected against hacker attacks, when in fact it is not.

Information security management, internal control and IT governance follows in importance as general response to hacking (most respondents agreed to a large extent or to a moderate extent), indicating that these are common responses in most banks. Software development practices were also rated fairly low as a response to hacking. Secure software development is essential to withstanding attacks by hackers (as discussed in sections 5.8.2 and 5.8.5). A lack thereof could lead to vulnerable software, which could be attacked by hackers.

Not all the company secretaries knew whether ethical hacking is used as a response to hacking (27%, with varied responses according to the highest standard deviation score of 1.68). Based on the responses from the company secretaries, ethical hacking is either not discussed, or is unknown or misunderstood at the board of directors level at some banks. Considering that ethical hacking has been highlighted as the most comprehensive response to hacking (as presented in Table 6.5), it is of concern that the responses from the company secretaries suggest that the banking sector does not use it more extensively as a response to the hacking threat. Company secretaries are either not familiar with the ethical hacking response, or they might not know how to apply the ethical hacking response. As a consequence, they cannot advise the board of directors accordingly.

Frameworks such as ITIL and CobiT have been ranked low as possible responses, which indicate that these frameworks do not feature prominently in the banking sector. It should be considered that a framework such as CobiT enables IT governance (Table 5.1) and is referred to in King III (IoD, 2009b:16). The company secretaries ranking IT governance as the third response indicate that the company secretaries may be over-confident in their IT governance practices, or they may be either informal or non-existent. Corporate governance has been ranked fairly low as a response. It also indicates that most likely company secretaries do not understand how corporate governance can be applied as a response to hacking.
Although security technologies have been ranked first (see Table 9.15) by company secretaries, none of the annual reports highlighted security technologies as a response to IT risk or hacking (Table 7.8). Ethical hacking was highlighted as one of the most comprehensive responses to hacking in this thesis (Table 6.5). Despite this, ethical hacking was not disclosed in any of the annual reports (Table 7.8), which supports the relative lack of knowledge that may exist regarding ethical hacking as a response to hacking (27% did not know whether ethical hacking was used as a response, further supported by the highest standard deviation score of 1.68, which supports the varied responses). Similarly, the low ranking of CobiT and ITIL (see Table 9.15) corresponds with the low disclosure of CobiT and ITIL in the annual reports (Table 7.8). ITIL is not an effective response to hacking; however, CobiT is a more effective response and could be considered as a response to IT risk. There is clearly a lack of disclosure of responses to threats, such as hacking, in the annual reports and a lack of understanding by company secretaries.

Table 9.16 The company secretaries’ views on the effectiveness of general responses to the risk of hacking in their organisation (own calculation from company secretary questionnaires) (n = 15)

<table>
<thead>
<tr>
<th>The effectiveness of general responses to hacking</th>
<th>Agree completely</th>
<th>Agree to a large extent</th>
<th>Agree to a moderate extent</th>
<th>Agree to a lesser extent</th>
<th>Don’t agree at all</th>
<th>Weighted arithmetic mean</th>
<th>Mean</th>
<th>Standard deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security technologies, such as firewalls.</td>
<td>10</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>4.07</td>
<td>1.93</td>
<td>1.62</td>
</tr>
<tr>
<td>Information security management.</td>
<td>8</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>3.87</td>
<td>2.13</td>
<td>1.60</td>
</tr>
<tr>
<td>Internal control.</td>
<td>7</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>3.80</td>
<td>2.20</td>
<td>1.57</td>
</tr>
<tr>
<td>IT governance.</td>
<td>7</td>
<td>3</td>
<td>2</td>
<td>0</td>
<td>3</td>
<td>3.73</td>
<td>2.27</td>
<td>1.58</td>
</tr>
<tr>
<td>Risk management.</td>
<td>6</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>3</td>
<td>3.67</td>
<td>2.33</td>
<td>1.54</td>
</tr>
<tr>
<td>Software development practices.</td>
<td>6</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>3.53</td>
<td>2.47</td>
<td>1.60</td>
</tr>
<tr>
<td>Corporate governance.</td>
<td>4</td>
<td>5</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>3.33</td>
<td>2.67</td>
<td>1.54</td>
</tr>
<tr>
<td>Ethical hacking.</td>
<td>5</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>6</td>
<td>3.00</td>
<td>3.00</td>
<td>1.85</td>
</tr>
<tr>
<td>Governance frameworks, such as CobiT.</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>5</td>
<td>3.00</td>
<td>3.00</td>
<td>1.65</td>
</tr>
<tr>
<td>Applying service and quality management, such as ITIL.</td>
<td>4</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>5</td>
<td>2.93</td>
<td>3.07</td>
<td>1.67</td>
</tr>
</tbody>
</table>

From the company secretaries’ perspective, security technologies such as firewalls have been listed as the most effective response to hacking in their organisation. Ironically, as presented in Table 5.4, security technologies do not address all the IT risk themes. Security technologies (effectively a component of information security management) are often the tactical response to hacking attacks and are perhaps also a well-known response to hacker attacks. As already mentioned, security technologies do not provide a comprehensive response to the hacking risk. Similarly, as presented in Table 5.4, information security management does not address all the IT risk themes. In contrast, ethical hacking, which has been argued as being the most effective response to any of the other responses in section...
6.14, has been ranked in eighth position by company secretaries. Six company secretaries (40%) indicated that they do not know whether ethical hacking is an effective response or not in their organisation (further supported by the highest standard deviation score of 1.85). This illustrates that ethical hacking and how it is used within the banking sector is not well known among the company secretaries. If the company secretaries do not understand how this is applied in their organisation, it follows that they will not be in a position to guide the board of directors to consider it as a possible response.

According to the company secretaries, software development practices are only effectively applied by some banks, which indicate that insecure software may exist within the banking sector. The varied response for corporate governance indicates that it is not clear to the company secretaries how hacking should be addressed from a corporate governance perspective. Respondents were correct in rating service and quality management as low, since this study has also argued that these are not effective responses to the IT risk of hacking. It can also be argued that the results show that they understand that a varied approach should be used.

9.2.10 The company secretaries’ views on the disclosure of IT

9.2.10.1 Objective of the question

The purpose of the eleventh set of questions was to obtain a view on IT disclosure practices in the organisation, specifically in relation to the organisation’s annual results (Question 11).

9.2.10.2 Findings and deductions

Company secretaries are responsible for the preparation of the integrated annual report (highlighted in section 8.5.1). Most company secretaries agreed (80%) that there is clear guidance available in terms of what should be included in the annual results from an IT governance perspective. Most company secretaries (80%) were of the opinion that their disclosure of IT governance was adequate.

<table>
<thead>
<tr>
<th>The company secretaries’ views on IT disclosure</th>
<th>Yes</th>
<th>%</th>
<th>No</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>There is clear guidance available on what should be reported in the annual results from an IT governance perspective.</td>
<td>12</td>
<td>80%</td>
<td>3</td>
<td>20%</td>
</tr>
<tr>
<td>IT governance-related disclosure in our most recent annual report is adequate.</td>
<td>12</td>
<td>80%</td>
<td>3</td>
<td>20%</td>
</tr>
</tbody>
</table>
The company secretaries' views on IT disclosure

<table>
<thead>
<tr>
<th>IT governance-related disclosure will increase in our future annual reports.</th>
<th>Yes</th>
<th>%</th>
<th>No</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>80%</td>
<td>3</td>
<td>20%</td>
<td></td>
</tr>
</tbody>
</table>

However, most company secretaries indicated that their disclosure of IT governance will increase in future annual reports but no further clarifying comments were provided regarding disclosure practices. These responses are in contradiction with the analysis of King III IT governance attributes presented in Table 7.4. Only half of the banks included details on IT governance attributes. It is noticeable that there is no consistency among banks in terms of what should be disclosed from an IT governance perspective, based on the analysis of the annual reports presented in Chapter 7.

9.2.11 Conclusion

The company secretary fulfils an essential corporate governance role in the banking sector. The questionnaires completed by the company secretaries highlighted various corporate governance practices and gave insight into the functioning of the board of directors in so far as IT matters are concerned.

It is evident from the questionnaires that the company secretaries feel that they are well supported by the board of directors. They are generally of the opinion that the board of directors takes its IT governance responsibilities seriously and that there is enough focus on IT risk, cybercrime and hacking. A few company secretaries have highlighted that their organisations might not be able to deal effectively with IT challenges such as recovering from hacker attacks.

The results from the questionnaires have highlighted that regulatory requirements were seen as the key driving factor behind the implementation of IT governance practices. Surprisingly, standards and frameworks do not play a vital role in establishing IT governance in the organisations, which indicates a lack of maturity in IT governance processes. Not all individuals responsible for IT are invited to the board of directors meetings. The responsibility for IT has been allocated to board members at only a few banks. This indicates that IT does not yet carry significance at the board of directors level. Generally, company secretaries are of the opinion that the individuals responsible for IT meet their strategic objectives. It is mostly non-board committees who deal with IT matters, emphasising that IT is probably only covered at a high level at most board of directors meetings. It is therefore unlikely that IT risks, such as hacking, would be a standing agenda point at meetings of boards of directors. Significant IT matters will find their way onto the agenda of boards of
The link between physical risk and IT risk is not well understood among the company secretaries and this may indicate that banks are probably underestimating the likelihood of social engineering attacks succeeding. Similarly, the extent to which IT risks such as IT human resources risk and lack of software development could be increased by hacking is not well understood by the company secretaries. Security technologies such as firewalls remain the traditional response to the risk of hacking, followed by internal control and IT governance, as indicated by the company secretaries. This thesis has argued that these responses are not the most effective in addressing IT risk. Despite the strong argument in favour of ethical hacking as a response, it scored relatively low as a response in the South African banking sector. The banking sector is therefore not sufficiently addressing IT risk and by implication not adequately protected against hacking, from the view of the company secretary, who is well positioned to have a view across the entire organisation. Frameworks and standards are not extensively used in the South African banking sector. Company secretaries were satisfied with the disclosure of IT governance, although the analysis of the annual reports showed inconsistencies in what is being reported from an IT governance perspective.

9.3 RESEARCH FINDINGS ON THE INDIVIDUAL RESPONSIBLE FOR IT

The section that follows documents the results of the questionnaires that were sent out to the individuals responsible for IT in the local banking sector.

9.3.1 The support that individuals responsible for IT get from their organisation

9.3.1.1 Objective of the question

The purpose of the first set of questions was to determine whether the individuals responsible for IT receive adequate support in their organisation, in particular from the board of directors (Question 1).

9.3.1.2 Findings and deductions

The following Likert scale was used by participants to rank the statements presented in Table 9.18: 1 = Agree completely; 2 = Agree to a large extent; 3 = Agree to a moderate
extent; 4 = Agree to a lesser extent; 5 = Don’t agree at all.

Table 9.18 The support that individuals responsible for IT get from their organisation (own calculation from the individual responsible for IT questionnaires) (n = 11)

| The support that individuals responsible for IT get from their organisation | Agree completely | Agree to a large extent | Agree to a moderate extent | Agree to a lesser extent | Don’t agree at all | n | Weighted arithmetic mean | Mean | Standard deviation |
|---|---|---|---|---|---|---|---|---|---|---|
| The board of directors supports me in my IT governance role. | 6 | 4 | 1 | 0 | 0 | 11 | 4.45 | 1.55 | 0.69 |
| I have sufficient resources to attend to IT governance. | 1 | 7 | 1 | 1 | 1 | 11 | 3.55 | 2.45 | 1.13 |
| The board of directors takes my views seriously. | 4 | 6 | 0 | 0 | 0 | 10* | 4.40 | 1.60 | 0.52 |
| I have sufficient opportunity to be heard at board committees. | 5 | 6 | 0 | 0 | 0 | 11 | 4.45 | 1.55 | 0.52 |

*One respondent did not rate this statement

King III encourages the appointment of a CIO to facilitate the interaction between the business and the board of directors on IT governance matters (as discussed in section 8.5.2). Most respondents (55% agreed completely and 36% agreed to a large extent) indicated that they received adequate support from the board of directors. Individuals responsible for IT agreed to a large extent (64%) that they have sufficient resources to effect IT governance. Regardless, the weighted arithmetic means for this question is low, indicating varied responses. One particular comment highlights that the necessary skill might be sourced somewhere else:

- “Securing permanent IT Governance resources and skills is difficult, we employ the services of specialised outsources such as PWC for these services.”

Most individuals responsible for IT (36% agreed completely and 55% agreed to a large extent) felt that they do have the opportunity to be heard by the board of directors. This result is further supported by a comment from one of the participants:

- “We have very formal and active board participation in IT governance, through an IT sub-committee. I also get involved at board meetings on Technology issues regarded as significant to the future of banking.”
9.3.2 The views of individuals responsible for IT on the board and IT governance

9.3.2.1 Objective of the question

The purpose of the set of statements included in the second question in the questionnaire was to determine the extent to which, in the view of those responsible for IT, the board of directors accepts its IT governance responsibilities. In addition, the importance of IT governance in the organisations was determined, as well as the board of director’s overall response to and awareness of IT risk, cybercrime and hacking (Question 2).

9.3.2.2 Findings and deductions

The following Likert scale was used by participants to rank the statements presented in Table 9.19: 1 = Agree completely; 2 = Agree to a large extent; 3 = Agree to a moderate extent; 4 = Agree to a lesser extent; 5 = Don’t agree at all.

It was established in section 5.6.4 that the board of directors carries the ultimate responsibility for IT governance. More than half of the respondents believe that the board of directors takes responsibility for IT governance (36% agree completely and 36% agree to a large extent). It is concerning to note even when IT is a critical enabler for banking operations, at least 18% of respondents felt that their board of directors does not take adequate responsibility for IT governance. The views expressed here are perhaps cautious, seeing that IT governance responsibilities are mostly delegated to other committees, as indicated in Table 9.10.

<table>
<thead>
<tr>
<th>Views on the board and IT governance</th>
<th>Agree completely</th>
<th>Agree to a large extent</th>
<th>Agree to a moderate extent</th>
<th>Agree to a lesser extent</th>
<th>Don’t agree at all</th>
<th>Weighted arithmetic mean</th>
<th>Mean</th>
<th>Standard deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>The board of directors takes responsibility for IT governance.</td>
<td>4</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>3.91</td>
<td>2.09</td>
<td>1.14</td>
</tr>
<tr>
<td>The board of directors effectively addresses IT governance.</td>
<td>3</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>3.73</td>
<td>2.27</td>
<td>1.10</td>
</tr>
<tr>
<td>The board members have the necessary skills to deal with IT matters.</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>3.18</td>
<td>2.82</td>
<td>1.08</td>
</tr>
<tr>
<td>IT governance is a key component of corporate governance in our organisation.</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>3.82</td>
<td>2.18</td>
<td>0.98</td>
</tr>
<tr>
<td>IT governance is high on the board’s agenda.</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>3.64</td>
<td>2.36</td>
<td>0.92</td>
</tr>
</tbody>
</table>
IT governance is important on the agenda of the board of directors at only some banks. Almost half of the respondents (9% agreed completely and 36% agreed to a large extent) believed the board members have sufficient skills to deal with IT matters. The weighted arithmetic means however highlights a mixed response, which remains an area of concern for some participants (36% agreed to a lesser extent), as expressed in the following quotes from individuals responsible for IT:

- “Although Board Members do not have all the IT background and skills they take an active interest in all things IT and Information related. The Board has established the necessary governance structures and actively participates.”
- “Here skills shortage at board level is a definite issue.”

The abovementioned indicates that the board members may not have the required skills to fulfil their IT responsibilities.

In terms of the importance of IT governance being placed on the agenda of the board of directors, the views were varied, ranging from agreeing completely, to not agreeing at all (supported by the low standard deviation score of 0.92, which indicates that the views are varied, rather than similar). The individuals responsible for IT are not in agreement regarding IT governance practices in the banking sector. Half of the respondents were of the opinion that their IT governance practices compare at least to a large extent (36% agreed completely and 18% agreed to a large extent) with their competitors. This implies that they take note of their competitors’ IT governance practices. However, at least two individuals responsible for IT indicated that their IT governance practices are not similar to other banks. Considering what was reported in the annual results of each bank (IT governance attributes highlighted in Table 7.4), it is not that apparent that IT governance practices are similar between banks. The response by the individuals responsible for IT might also indicate varied opinions regarding IT governance practices at the board of directors level.

Respondents gave exactly the same ratings to the statements about responses to
cybercrime and hacking. Respondents agreed to a large extent (9% agreed completely and 64% agreed to a large extent) that the board of directors’ overall response to IT risk, cybercrime and hacking was good. This could be an indication that respondents view these as related or as a sub-set of each other. At least two banks were not so confident that their board of directors responds adequately to IT risk, cybercrime or hacking. This indicates that some banks could be at risk of being successfully attacked by hackers, due to their inability to respond adequately to hacker attacks.

9.3.3 The views of the individuals responsible for IT on IT in business

9.3.3.1 Objective of the question

The third question in the questionnaire comprised statements that were aimed at determining the general position of IT in supporting business, as a precursor to some of the more specific questions that followed in the remainder of the questionnaire (Question 3).

9.3.3.2 Findings and deductions

The following Likert scale was used by participants to rank the statements presented in Table 9.20: 1 = Agree completely; 2 = Agree to a large extent; 3 = Agree to a moderate extent; 4 = Agree to a lesser extent; 5 = Don’t agree at all.

Table 9.20 The views of individuals responsible for IT on IT in business (own calculation from the individual responsible for IT questionnaires) (n = 11)

<table>
<thead>
<tr>
<th>The views of the individuals responsible for IT on IT in business</th>
<th>Agree completely</th>
<th>Agree to a large extent</th>
<th>Agree to a moderate extent</th>
<th>Agree to a lesser extent</th>
<th>Don’t agree at all</th>
<th>Weighted arithmetic mean</th>
<th>Mean</th>
<th>Standard deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our ability to deal with IT challenges is good.</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>4.00</td>
<td>2.00</td>
<td>0.77</td>
</tr>
<tr>
<td>Our ability to deal with IT risk is good.</td>
<td>2</td>
<td>5</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>3.82</td>
<td>2.18</td>
<td>0.75</td>
</tr>
<tr>
<td>IT plays a key enabling role in our products and services.</td>
<td>5</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>4.27</td>
<td>1.73</td>
<td>0.90</td>
</tr>
<tr>
<td>Our IT governance practices are key to fighting cybercrime.</td>
<td>1</td>
<td>7</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3.82</td>
<td>2.18</td>
<td>0.60</td>
</tr>
</tbody>
</table>

Nearly all individuals responsible for IT agree that IT plays a key enabling role in their organisation’s products and services (45% agreed completely and 45% agreed to a large extent). It has been argued in this thesis that IT brings with it significant risk. The CIO has a shared responsibility for risk management, as established in section 5.4.5, which includes
the management of IT risk. Five respondents (45%) agreed to a large extent that their ability to deal with IT risk is good, although some respondents were not so confident (36% agreed to a lesser extent). Respondents were of the opinion that their ability to deal with IT challenges ranged from a moderate extent to completely able. The responses regarding the banks’ ability to deal with IT challenges and IT risk were varied, indicating that the individuals responsible for IT were not all confident in their organisation’s ability to deal with IT challenges and IT risk. The CIO is responsible for enabling IT governance in the organisation (highlighted in sections 5.6.4 and 8.5.2). IT governance practices have been seen as key to fighting cybercrime from a moderate to a large extent (9% agreed complete, 64% agreed to a large extent and 27% agreed to a moderate extent, also supported by the lowest standard deviation score of 0.60 in Table 9.20). There were no further comments by the individuals responsible for IT. The relatively low score for the last statement in Table 9.20 indicates that not enough emphasis is placed on the organisation’s IT governance practices, which includes the participation of the board of directors in the response to cybercrime. The results also indicate that most banks will be able to respond to hacker attacks, while a few banks might find it difficult to respond adequately or obtain support from the board of directors. The individuals responsible for IT at some banks can do more to ensure that their IT governance processes are mature enough to respond to hacker attacks and to seek participation from the board of directors.

9.3.4 The views of the individuals responsible for IT on incorporating IT governance into their organisation

9.3.4.1 Objective of the question

The objective of the fourth question was to determine the views of the individuals responsible for IT on the factors which drive the implementation of IT governance in their organisation, by way of a ranking of pre-determined factors (Question 4).

9.3.4.2 Findings and deductions

In Question 4, respondents were asked to rank five key drivers towards incorporating IT governance into their organisation. The results in Table 9.21 were ranked in descending order according to the weighted arithmetic mean. One respondent ranked two statements in first position and left out the fourth ranking.
Table 9.21  The views of the individuals responsible for IT on incorporating IT governance into their organisation (own calculation from the questionnaires of individuals responsible for IT)

<table>
<thead>
<tr>
<th>Views on incorporating IT governance into the organisation</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
<th>4th</th>
<th>5th</th>
</tr>
</thead>
<tbody>
<tr>
<td>Achieving business objectives or strategy.</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Regulatory requirements or legislation.</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Growth in complexity of the IT function.</td>
<td>3</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>The culture of the organisation.</td>
<td>2</td>
<td>0</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Industry norm and practice.</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>5</td>
<td>4</td>
</tr>
</tbody>
</table>

Figure 9.2  The views of the individuals responsible for IT on incorporating IT governance into their organisation (own presentation)

The CIO plays a role in enabling IT governance and aligning IT strategy and objectives with the organisation’s business objectives (discussed in section 8.5.2). Overall, achieving business objectives or strategy has been rated as the primary reason for incorporating IT governance, which is in line with the objectives of IT governance in general (as discussed in section 5.6.1). Regulatory requirements or legislation has been ranked as the second most important reason behind incorporating IT governance into the organisation. A possible reason behind this might be the introduction of IT governance in King III. Industry norm and practice has been ranked last (also supported by the lowest weighted arithmetic mean score of 1.91), which indicates that IT governance is regarded as a valid discipline and not followed simply because competitors choose to follow IT governance practices. However, this also indicates that best practice frameworks do not carry significant weight at most banks from the perspective of the individual responsible for IT.
9.3.5 The individuals responsible for IT’s view on business risk and IT risk

9.3.5.1 Objective of the question

The objective of the fifth question was to determine to what extent the individual responsible for IT believes that IT risk increases each of the business risks presented in this thesis. This will provide the view of the individual responsible for IT on the pervasive nature of IT risk (Question 5).

9.3.5.2 Findings and deductions

The following Likert scale was used by participants to rank the statements presented in Table 9.22: 1 = To a large extent; 2 = To a moderate extent; 3 = To a small extent; 4 = Not at all. The results in Table 9.22 were ranked in descending order according to the weighted arithmetic mean.

The CIO has a key responsibility in participating in the organisation’s risk management processes, in particular where IT risk is of concern (as discussed in section 5.4.5). Disaster recovery risk received the highest ranking (82% agreed to a large extent and 18% to a moderate extent), which is an indication of the importance of continuity of business operations for the organisation.

Table 9.22 The views of the individuals responsible for IT on business risk and IT risk (own calculation from the questionnaires of individuals responsible for IT) (n = 11)

<table>
<thead>
<tr>
<th>IT risk linked to business risk</th>
<th>To a large extent</th>
<th>To a moderate extent</th>
<th>To a small extent</th>
<th>Not at all</th>
<th>Weighted arithmetic mean</th>
<th>Mean</th>
<th>Standard deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disaster recovery risk.</td>
<td>9</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>3.82</td>
<td>1.18</td>
<td>0.40</td>
</tr>
<tr>
<td>Technology risk.</td>
<td>9</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>3.73</td>
<td>1.27</td>
<td>0.65</td>
</tr>
<tr>
<td>Operational risk.</td>
<td>8</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3.73</td>
<td>1.27</td>
<td>0.47</td>
</tr>
<tr>
<td>Business continuity risk.</td>
<td>8</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3.73</td>
<td>1.27</td>
<td>0.47</td>
</tr>
<tr>
<td>Reputational risk.</td>
<td>7</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>3.55</td>
<td>1.45</td>
<td>0.69</td>
</tr>
<tr>
<td>Compliance risk.</td>
<td>4</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>3.27</td>
<td>1.73</td>
<td>0.65</td>
</tr>
<tr>
<td>Credit risk.</td>
<td>4</td>
<td>5</td>
<td>2</td>
<td>0</td>
<td>3.18</td>
<td>1.82</td>
<td>0.75</td>
</tr>
<tr>
<td>Human resource risk.</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>0</td>
<td>3.00</td>
<td>2.00</td>
<td>0.77</td>
</tr>
<tr>
<td>Market risk.</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>0</td>
<td>3.00</td>
<td>2.00</td>
<td>0.77</td>
</tr>
<tr>
<td>Physical risk.</td>
<td>1</td>
<td>5</td>
<td>5</td>
<td>0</td>
<td>2.64</td>
<td>2.36</td>
<td>0.67</td>
</tr>
</tbody>
</table>

Technology risk closely follows disaster recovery risk. Respondents were of the view that these are strongly linked to IT risk, which is perhaps not surprising, seeing that these are
concepts strongly related to IT in general. Implicitly the respondents agreed that hackers directly threaten organisations’ technology and their ability to continue operations (the strong link with hacking was highlighted in sections 4.8 and 4.9). Reputational risk received a high rating and individuals responsible for IT were clearly concerned about the impact of IT risk on the organisation’s reputational risk (as discussed in section 4.12). Operational risk has been recognised by at least eight respondents (73% agreed to a large extent) as a risk that could be affected by IT risk (as discussed in section 4.6). The individuals responsible for IT do not see a strong link between market risk and IT risk, despite the fact that 94% of the banks disclosed market risk in their annual reports (Table 7.6). The same applies to compliance risk (disclosed by all banks) and credit risk (disclosed by 94% of the banks). The responses for human resource risk and market risk were varied, with the highest standard deviation scores of 0.77 each. The links between human resource risk, physical risk and IT risk are not well understood by the individuals responsible for IT and have been ranked lower. This also indicates that respondents underestimate the impact IT risk could have on these risks. In particular the low rating of physical risk implies that respondents do not understand the risk associated with hackers and their physical entry into a bank’s premises by applying social engineering techniques (as discussed in section 3.8.3.1). There were no clarifying comments provided the individuals responsible for IT. Seeing that the individuals responsible for IT do not fully realise the impact IT risk has on all of the business risks, they might fail to respond adequately to the IT risks (such as hacking) which may threaten each bank.

9.3.6 The views of the individuals responsible for IT on hacking

9.3.6.1 Objective of the question

The objective of the sixth question was to determine the views of the individuals responsible for IT on the significance of hacking in their organisations. The statements presented in Table 9.23 range from hacking being recognised as a risk, to testing awareness of hacker characteristics (Question 6).

9.3.6.2 Findings and deductions

The following Likert scale was used by participants to rank the statements presented in Table 9.20: 1 = Agree completely; 2 = Agree to a large extent; 3 = Agree to a moderate extent; 4 = Agree to a lesser extent; 5 = Don’t agree at all.
Table 9.23  The views of the individuals responsible for IT on hacking (own calculation from the questionnaires of individuals responsible for IT) (n = 11)

<table>
<thead>
<tr>
<th>The views of the individual responsible for IT on hacking</th>
<th>Agree completely</th>
<th>Agree to a large extent</th>
<th>Agree to a moderate extent</th>
<th>Agree to a lesser extent</th>
<th>Don't agree at all</th>
<th>Weighted arithmetic mean</th>
<th>Mean</th>
<th>Standard deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacking is a significant risk in our organisation.</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>3.82</td>
<td>2.18</td>
<td>1.47</td>
</tr>
<tr>
<td>As an organisation, we are responsible for client-side security against hacking.</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>3.27</td>
<td>2.73</td>
<td>1.49</td>
</tr>
<tr>
<td>As an organisation, we should take responsibility for phishing attacks against clients.</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>3.55</td>
<td>2.45</td>
<td>1.13</td>
</tr>
<tr>
<td>Hacking is on the board’s agenda.</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3.18</td>
<td>2.82</td>
<td>1.54</td>
</tr>
<tr>
<td>Hacking significantly increases our organisation’s reputational risk.</td>
<td>6</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>4.36</td>
<td>1.64</td>
<td>0.92</td>
</tr>
<tr>
<td>Hacking is a perceived risk as opposed to a real risk.</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>7</td>
<td>1.73</td>
<td>4.27</td>
<td>1.27</td>
</tr>
<tr>
<td>Our protection against hacker attacks from inside the organisation is good.</td>
<td>1</td>
<td>5</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>3.27</td>
<td>2.73</td>
<td>1.19</td>
</tr>
<tr>
<td>Hacking should be prevented.</td>
<td>5</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>4.27</td>
<td>1.73</td>
<td>0.79</td>
</tr>
<tr>
<td>Hacking should be detected.</td>
<td>8</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>4.64</td>
<td>1.36</td>
<td>0.67</td>
</tr>
<tr>
<td>The skills level of a hacker affects the response to his attacks.</td>
<td>3</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>3.55</td>
<td>2.45</td>
<td>1.37</td>
</tr>
<tr>
<td>The moral viewpoint of a hacker affects the response to his attacks.</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>2.00</td>
<td>4.00</td>
<td>1.34</td>
</tr>
<tr>
<td>Our risk of hacker attack from inside the organisation is greater than the external risk.</td>
<td>3</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>3.55</td>
<td>2.45</td>
<td>1.13</td>
</tr>
</tbody>
</table>

As part of the CIO’s risk management responsibilities (highlighted in section 8.5.2), the CIO should recognise the importance of addressing the IT risk of hacking. Most respondents agree completely (55%) that hacking is a significant risk for their organisation and not simply a perceived risk. Most respondents agree completely (73%) that hacking should be detected, but somewhat fewer (45% agree completely and 36% agree to a large extent) that hacking should be prevented. The responses from the individuals responsible for IT varied in terms of the statement regarding the responsibility for client-side security against hacking (supported by a fairly high standard deviation value of 1.49). Slightly more participants agreed to a large extent (18% agreed completely and 36% agreed to a large extent) that their banking clients need to be protected against phishing attacks. Not all participants agreed that hacker attacks from inside the organisation are greater than the risk of external attacks. This perception might be the reason why more than half of the respondents indicated that their controls inside the organisation against hacker attacks are adequate (45% agreed to a large extent). The risk of insider attack is therefore not clearly understood, which is of particular concern given that the literature study (section 3.5.3.6) highlighted that the risk of internal attacks is at times higher than the risk of external attacks.
Hacking is on the agenda of the board of directors at only some of the banks (27% agreed completely and 18% agreed to a large extent). The ranking of this statement varies, as indicated by the highest standard deviation value in Table 9.23. This despite the fact that most respondents (55% agreed completely and 36% to a large extent) were of the opinion that reputational risk may be affected by hacker attacks. This further supports the findings reported in Table 9.10, which indicates that IT matters are delegated to other management committees, rather than dealt with directly by the board of directors.

At least half of the respondents (55%) did not agree that the moral viewpoints of hackers affect the response to hacker attacks. This despite the prevalence of hactivism attacks (as discussed in section 3.5.3.2), which requires increased vigilance by the banking sector. This also indicates that respondents do not understand some of the fundamental characteristics of hackers and what drives them to launch attacks against banks. Most respondents agreed at least to a large extent (27% and 36% agreed completely) that the skills level of a hacker will affect the response required.

The focus of Table 9.24 was to determine how hacking increases the some of the IT risk themes identified in this thesis. The following Likert scale was used by participants to rank the statements presented in Table 9.24: 1 = To a large extent; 2 = To a moderate extent; 3 = To a small extent; 4 = Not at all. The results were ranked in descending order according to the weighted arithmetic mean.

<table>
<thead>
<tr>
<th>Hacking increasing the IT risks below</th>
<th>To a large extent</th>
<th>To a moderate extent</th>
<th>To a small extent</th>
<th>Not at all</th>
<th>n</th>
<th>Weighted arithmetic mean</th>
<th>Mean</th>
<th>Standard deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical access risk.</td>
<td>8</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>11</td>
<td>3.73</td>
<td>1.27</td>
<td>0.47</td>
</tr>
<tr>
<td>IT continuity risk.</td>
<td>8</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>11</td>
<td>3.64</td>
<td>1.36</td>
<td>0.67</td>
</tr>
<tr>
<td>Cybercrime.</td>
<td>6</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>11</td>
<td>3.55</td>
<td>1.45</td>
<td>0.52</td>
</tr>
<tr>
<td>IT systems risk.</td>
<td>6</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>11</td>
<td>3.36</td>
<td>1.64</td>
<td>0.92</td>
</tr>
<tr>
<td>IT non-compliance risk.</td>
<td>3</td>
<td>7</td>
<td>1</td>
<td>0</td>
<td>11</td>
<td>3.18</td>
<td>1.82</td>
<td>0.60</td>
</tr>
<tr>
<td>IT human resources risk.</td>
<td>4</td>
<td>4</td>
<td>3</td>
<td>0</td>
<td>11</td>
<td>3.09</td>
<td>1.91</td>
<td>0.83</td>
</tr>
<tr>
<td>Physical access risk.</td>
<td>2</td>
<td>7</td>
<td>2</td>
<td>0</td>
<td>11</td>
<td>2.90</td>
<td>2.00</td>
<td>0.63</td>
</tr>
<tr>
<td>Communications failure.</td>
<td>4</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td>11</td>
<td>2.91</td>
<td>2.09</td>
<td>1.14</td>
</tr>
<tr>
<td>Lack of software development.</td>
<td>2</td>
<td>2</td>
<td>5</td>
<td>1</td>
<td>10</td>
<td>2.50</td>
<td>2.50</td>
<td>0.97</td>
</tr>
</tbody>
</table>

*One respondent did not choose an option

Almost all respondents agreed to a large extent (73%) that hacking will increase the logical access risk. IT continuity risk has been ranked second (73% agreed to a large extent and
18% agreed to a moderate extent).

*Lack of software development* and *communication failure* received varied responses from participants (reflected by the lowest weighted arithmetic mean scores). Respondents did not consider that poor software development practices may introduce software vulnerabilities that may be exploited by hackers (discussed in section 3.8.5). Some respondents are completely unaware (18% indicate not at all) of how DoS attacks by hackers could significantly increase the risk of *communication failure* (highlighted in sections 3.3.2 and 3.5.3.1). It is important to reflect on the close link between hacking and all the IT risk themes identified in this thesis (as presented in Table 4.30). It follows that the individuals responsible for IT do not recognise the link between hacking and the IT risk themes and how they can be clearly affected by hackers.

**Table 9.25** The views of the individuals responsible for IT on the effectiveness of hacker responses (own calculation from the questionnaires of individuals responsible for IT) (n = 11)

<table>
<thead>
<tr>
<th>Effectiveness of hacker responses</th>
<th>Very Good</th>
<th>Good</th>
<th>Fair</th>
<th>Poor</th>
<th>Very Poor</th>
<th>Weighted arithmetic mean</th>
<th>Mean</th>
<th>Standard deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical response.</td>
<td>4</td>
<td>3</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>4.00</td>
<td>2.00</td>
<td>0.89</td>
</tr>
<tr>
<td>Technical response.</td>
<td>2</td>
<td>8</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>4.09</td>
<td>1.91</td>
<td>0.54</td>
</tr>
<tr>
<td>Employee vigilance.</td>
<td>1</td>
<td>5</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>3.64</td>
<td>2.36</td>
<td>0.67</td>
</tr>
<tr>
<td>Overall response.</td>
<td>1</td>
<td>6</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>3.73</td>
<td>2.27</td>
<td>0.65</td>
</tr>
</tbody>
</table>

In terms of the physical response to hacker attacks, the individuals responsible for IT rated their responses evenly in the range fair to very good. In general, it is expected that banks will have strong physical security, seeing that they are the custodians of public money. However, from the responses to this question, participating banks effectively admit that their physical response to hacking can improve (36% only rated it as fair). Most respondents have indicated that their technical response is good (73%). Again, if it is considered that most of the participating banks will have Internet banking or payment facilities, the expectation would be that the technical response should be very good. If it is not at that level, hacker attacks may be successful. Nonetheless, one bank’s comment highlighted why hacking responses may not be a necessity for them:

- “As we are not a retail bank with no transactional web access, the hacking risk is very low”.

Evidently, this respondent has not considered the risk of internal attacks.
Employee vigilance is fair (45%) to good (45%) and rated the lowest of the three response types. This also indicates that hacker attacks, both external and in particular internal, may simply go unnoticed. More than half of the individuals responsible for IT rated their overall response to hacking as good (55% and 9% very good), which indicates that they are confident to some extent in their responses to hacking.

Turning to factors which increase hacking, the results in Table 9.26 are ranked in descending order according to the weighted arithmetic mean.

Criminal awareness of the success of hacking has been ranked the highest factor in increasing the risk of hacking in the banking sector and highlights that the individuals responsible for IT are clearly aware of the growing threat of cybercrime. The general accessibility of hacking tools is also considered a significant contributing factor to the increase of hacking.

Table 9.26  The views of the individuals responsible for IT on factors which increases hacking in the banking sector (own calculation from the questionnaires of individuals responsible for IT) (n = 11)

<table>
<thead>
<tr>
<th>Factors which increase hacking in the banking sector</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
<th>4th</th>
<th>5th</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criminal awareness of the success of hacking.</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>General accessibility of hacking tools.</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Dependency of the public on mobile devices (e.g. smartphones).</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Dependency of the public on computers.</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Ease of entry into hacking (free books, online tutorials, cheaper bandwidth).</td>
<td>0</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

Figure 9.3  The views of the individuals responsible for IT on factors which increase hacking in the banking sector (own presentation)
The dependency of the public on mobile devices has been ranked third and also higher than the dependency of the public on computers. This indicates that the individuals responsible for IT are aware that hacker attacks evolve alongside technology, such as mobile devices, as highlighted in section 3.8.3.2. Respondents did not consider the ease of entry into hacking as a significant contributing factor (supported by the high weighted arithmetic mean of 2.55).

9.3.7 The views of the individual responsible for IT on responses to hacking

9.3.7.1 Objective of the question

The purpose behind the seventh question was to focus on the responses to hacking identified in this thesis in order to determine if these are being used in the banking sector, and, secondly, to determine which of these are deemed to be the most effective (Question 7).

9.3.7.2 Findings and deductions

The following Likert scale was used by participants to rank the statements presented in Table 9.27 and Table 9.28: 1 = Agree completely; 2 = Agree to a large extent; 3 = Agree to a moderate extent; 4 = Agree to a lesser extent; 5 = Don’t agree at all. The results in Table 9.27 were ranked in descending order according to the weighted arithmetic mean.

Table 9.27 The views of the individuals responsible for IT on the responses to hacking in their organisation (own calculation from the questionnaires of individuals responsible for IT) (n = 11)

<table>
<thead>
<tr>
<th>Responses to hacking being used</th>
<th>Agree completely</th>
<th>Agree to a large extent</th>
<th>Agree to a moderate extent</th>
<th>Agree to a lesser extent</th>
<th>Don’t agree at all</th>
<th>Weighted arithmetic mean</th>
<th>Mean</th>
<th>Standard deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information security management.</td>
<td>9</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4.82</td>
<td>1.18</td>
<td>0.40</td>
</tr>
<tr>
<td>Security technologies, such as firewalls.</td>
<td>8</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4.73</td>
<td>1.27</td>
<td>0.47</td>
</tr>
<tr>
<td>IT governance.</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4.45</td>
<td>1.55</td>
<td>0.52</td>
</tr>
<tr>
<td>Risk management.</td>
<td>4</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>4.27</td>
<td>1.73</td>
<td>0.65</td>
</tr>
<tr>
<td>Internal control.</td>
<td>4</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>4.27</td>
<td>1.73</td>
<td>0.65</td>
</tr>
<tr>
<td>Applying service and quality management, such as ITIL.</td>
<td>1</td>
<td>9</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>3.91</td>
<td>2.09</td>
<td>0.70</td>
</tr>
<tr>
<td>Software development practices.</td>
<td>3</td>
<td>5</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>3.73</td>
<td>2.27</td>
<td>1.27</td>
</tr>
<tr>
<td>Governance frameworks, such as CobiT.</td>
<td>1</td>
<td>7</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>3.73</td>
<td>2.27</td>
<td>0.79</td>
</tr>
<tr>
<td>Ethical hacking.</td>
<td>2</td>
<td>5</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>3.64</td>
<td>2.36</td>
<td>1.03</td>
</tr>
<tr>
<td>Corporate governance.</td>
<td>0</td>
<td>7</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>3.45</td>
<td>2.55</td>
<td>0.82</td>
</tr>
</tbody>
</table>
The CIO should be familiar with various responses to hacking, such as risk management (section 5.4.5), internal control (section 5.5.4), IT governance (section 5.6.4), information security management (section 5.9.7) and ethical hacking (section 6.13). The CIO also facilitates the link between business and IT. This is accomplished via IT governance, which also facilitates the link with corporate governance, as discussed in section 8.5.2. The survey results show that information security management and security technologies have been ranked as the most common responses to hacking by the participants (also supported by the lowest standard deviation values of 0.40 and 0.47, which indicates similar responses between respondents). These are followed by IT governance and risk management. The governance framework CobiT was ranked third last, despite being specifically mentioned in King III (IoD, 2009b:16). This indicates that the individuals responsible for IT have not applied governance frameworks as a response to hacking in their respective organisation.

Ethical hacking is ranked the second last response to hacking, with varied responses by the participants (also reflected by the high standard deviation score of 1.03). This indicates that there is no consistency in the banking sector in terms of the use of ethical hacking as a response to hacking. The individual responsible for IT should be a primary advocate of the use of ethical hacking as a response to hacking. This is clearly not evident in the South African banking sector. Corporate governance has been ranked last, which indicates that the individuals responsible for IT are themselves unsure how corporate governance can be applied as a response to hacking. There was a preference for detective rather than preventative responses to hacking, as highlighted by the individuals responsible for IT (Table 9.23). This provides a possible explanation as to why ethical hacking and software development practices are rated low as responses, since these are preventative responses.

The effectiveness of responses to hacking, from the individuals responsible for IT perspective was identified in Table 9.28. The results were ranked in descending order according to the weighted arithmetic mean.

Security technologies and information security management have been highlighted by those responsible for IT in the banks as the most effective responses to hacking. Security technologies such as firewalls are often the most immediate and preventative response to hacking (supported by the low standard deviation value of 0.50). Firewalls might be effective in preventing the general everyday attacks by less skilled hackers; however they will not prevent skilled hackers from breaking into the organisation. Nonetheless, this does indicate that banks require a tactical response to the immediate threat of hackers. Ethical hacking has been ranked as the eighth effective response type to hacking. Similar to the results in
Table 9.27, the responses were varied (as indicated by the high standard deviation values).

Table 9.28  The views of the individuals responsible for IT on the effectiveness of responses to hacking (own calculation from the questionnaires of individuals responsible for IT) (n = 11)

<table>
<thead>
<tr>
<th>Effectiveness of responses being used</th>
<th>Agree completely</th>
<th>Agree to a large extent</th>
<th>Agree to a moderate extent</th>
<th>Agree to a lesser extent</th>
<th>Don't agree at all</th>
<th>Weighted arithmetic mean</th>
<th>Mean</th>
<th>Standard deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security technologies, such as firewalls.</td>
<td>7</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4.64</td>
<td>1.36</td>
<td>0.50</td>
</tr>
<tr>
<td>Information security management.</td>
<td>6</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>4.45</td>
<td>1.55</td>
<td>0.69</td>
</tr>
<tr>
<td>Internal control.</td>
<td>2</td>
<td>7</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>4.00</td>
<td>2.00</td>
<td>0.63</td>
</tr>
<tr>
<td>Risk management.</td>
<td>2</td>
<td>6</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3.91</td>
<td>2.09</td>
<td>0.70</td>
</tr>
<tr>
<td>IT governance.</td>
<td>2</td>
<td>5</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>3.82</td>
<td>2.18</td>
<td>0.75</td>
</tr>
<tr>
<td>Corporate governance.</td>
<td>2</td>
<td>5</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>3.73</td>
<td>2.27</td>
<td>0.90</td>
</tr>
<tr>
<td>Software development practices.</td>
<td>2</td>
<td>6</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>3.64</td>
<td>2.36</td>
<td>1.21</td>
</tr>
<tr>
<td>Ethical hacking.</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>0</td>
<td>3.55</td>
<td>2.45</td>
<td>1.04</td>
</tr>
<tr>
<td>Applying service and quality management, such as ITIL.</td>
<td>0</td>
<td>6</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>3.45</td>
<td>2.55</td>
<td>0.69</td>
</tr>
<tr>
<td>Governance frameworks, such as CobiT.</td>
<td>0</td>
<td>5</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>3.27</td>
<td>2.73</td>
<td>0.79</td>
</tr>
</tbody>
</table>

Ethical hacking has perhaps not yet been accepted in the banking sector as an effective response to hacking. Governance frameworks have been ranked last, which supports the results in Table 9.27, indicating that governance frameworks are not commonly used in the banking sector, again despite the fact that King III listed CobiT specifically (IoD, 2009b:16). There were no clarifying comments by the individuals responsible for IT. The results indicate that the banking sector is not deploying the most effective responses to hacking and may not be adequately protected against sophisticated hacker attacks.

9.3.8 The views of the individuals responsible for IT on ethical hacking

9.3.8.1 Objective of the question

The objective of the eighth question was to determine the use of ethical hacking as a response to hacking in the banking sector and also to consider the advantages and disadvantages associated with ethical hacking (Question 8).

9.3.8.2 Findings and deductions

The following Likert scale was used by participants to rank the statements presented in Table 9.29: 1 = To a large extent; 2 = To a moderate extent; 3 = To a small extent; 4 = Not at all.
Table 9.29 The views of the individuals responsible for IT on the effectiveness of ethical hacking as a response in their organisation (own calculation from the questionnaires of individuals responsible for IT) (n = 11)

<table>
<thead>
<tr>
<th>Effectiveness of ethical hacking as a response</th>
<th>To a large extent</th>
<th>To a moderate extent</th>
<th>To a small extent</th>
<th>Not at all</th>
<th>Weighted arithmetic mean</th>
<th>Mean</th>
<th>Standard deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you think that ethical hacking is an effective response to hacking in the bank?</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>13.45</td>
<td>1.55</td>
<td>0.52</td>
</tr>
</tbody>
</table>

The CIO is a role-player pertaining to the use ethical hacking (section 6.13). Approximately half of the respondents (45%) agreed to a large extent and half (55%) to a moderate extent that ethical hacking is an effective response to hacking in their organisation. This despite the fact that ethical hacking has not been highlighted as an effective response in their organisation (in Table 9.28, ethical hacking was ranked low).

Table 9.30 The views of the individuals responsible for IT on the use of ethical hacking (own calculation from individual responsible for IT questionnaires) (n = 11)

<table>
<thead>
<tr>
<th>Ethical hacking used within the bank</th>
<th>Yes</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Has your organisation ever made use of ethical hacking in the bank?</td>
<td>8</td>
<td>73%</td>
</tr>
</tbody>
</table>

Almost all respondents have made use of ethical hacking at some point. This indicates that ethical hacking is not an uncommon practice in the South African banking sector. It also indicates that ethical hacking is used at least to some extent to test organisations’ IT system defences. The results of Table 9.30 perhaps suggest that ethical hacking might be applied only to a limited extent in the banking sector due to a lack of knowledge on how to apply it effectively as a response to IT risk themes and hacking.

Respondents were asked to rank a number of factors which can be considered the disadvantages of ethical hacking, and the following table shows the results. The results have been sorted in descending order, according to the rankings.

Table 9.31 The views of the individuals responsible for IT on the disadvantages of ethical hacking (own calculation from the questionnaires of individuals responsible for IT) (n = 10)

<table>
<thead>
<tr>
<th>Disadvantages of ethical hacking</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
<th>4th</th>
</tr>
</thead>
<tbody>
<tr>
<td>The success of ethical hacking assignments depends on the skills level of the ethical hacker.</td>
<td>5</td>
<td>2</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Confidential information could be disclosed during an ethical hacking assignment.</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Banking systems may be affected by ethical hacking activity.</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>Ethical hacking results might be ambiguous and complex to remediate.</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>6</td>
</tr>
</tbody>
</table>
Only 10 participants completed this question, as one respondent indicated that he wished not to answer this question. Another respondent ranked two statements in third position and left the second position blank (rankings included unaltered). This result is visually represented in Figure 9.4. Most respondents were of the opinion that to ensure the successful outcome of ethical hacking assignments, the skills level of the ethical hacker will be a determining factor (50% ranked this statement in first position). This might also indicate that the individuals responsible for IT might not have been satisfied with the skills level available among ethical hackers. A high skills level could be defined as a specific requirement to an ethical hacking engagement when an external service provider is used (as discussed in section 6.6) and disclosure of ethical hacking qualifications, such as those discussed in section 6.7, could also be a prerequisite.

An organisation’s systems being affected by ethical hacking activity has been highlighted in sections 6.5.3, 6.11.1 and 6.11.3 as a disadvantage of ethical hacking. Surprisingly, the individuals responsible for IT were not particularly concerned that ethical hacking might have a negative effect on the bank’s systems. This could indicate that there is a good understanding that ethical hackers are mindful of how they affect the organisation’s systems and that some level of oversight is required over the ethical hacking activity. It could also indicate that ethical hackers are not allowed to perform their tests on the production system (they might be asked to perform their tests in the test environment, as highlighted in Table 6.1 and section 6.11.1). Respondents were also not concerned that ethical hacking results are too ambiguous to remediate (which was highlighted as a disadvantage in section 6.11.2).

**Figure 9.4** The views of the individuals responsible for IT on the disadvantages of ethical hacking (own presentation)
Respondents were further asked to rank a number of factors which can be considered the advantages of ethical hacking, and the results are shown in the following Table 9.32. The results have been sorted in descending order, according to the rankings.

Most respondents agreed that the main advantage of using ethical hacking is identifying and remediating information security and software vulnerabilities. Secondly, respondents were of the opinion that it is also used to test the effectiveness of internal control against hacker attacks.

Table 9.32 The views of the individuals responsible for IT on the advantages of ethical hacking (own calculation from the questionnaires of individuals responsible for IT) (n = 11)

<table>
<thead>
<tr>
<th>Advantages of ethical hacking</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
<th>4th</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify and remediate information security and software vulnerabilities.</td>
<td>5</td>
<td>4</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Test the effectiveness of internal control against hacker attacks.</td>
<td>3</td>
<td>4</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Avert potential reputational losses due to hacker attacks.</td>
<td>2</td>
<td>2</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>Persuade management of the threat of hacking.</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>8</td>
</tr>
</tbody>
</table>

Four respondents were not convinced that ethical hacking can be used to test internal control, which further indicates the lack of understanding among the individuals responsible for IT of the true nature of ethical hacking. Also, a high number of respondents (64% ranked it in third or fourth position) were unsure how ethical hacking can be used to avert reputational consequences. Almost all respondents (73% ranked it in fourth position) did not think ethical hacking should be used to persuade management of the threat of hacking. This could imply either that the threat of hacking is well known in the banking sector or that hacking has not yet been placed on the agenda of the board of directors for discussion.

Figure 9.5 The views of the individuals responsible for IT on the advantages associated with ethical hacking (own presentation)
This thesis has highlighted that a certain skills level and practical experience need to be demonstrated during the recruitment of an ethical hacker (as discussed in section 6.6).

Table 9.33 The views of the individuals responsible for IT on the use of unique recruitment practices when employing ethical hackers in their organisation (own calculation from the questionnaires of individuals responsible for IT) (n = 10)

<table>
<thead>
<tr>
<th>Unique recruitment practices when employing ethical hackers</th>
<th>Yes</th>
<th>%</th>
<th>No</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applying unique recruitment practices.</td>
<td>4</td>
<td>40%</td>
<td>6</td>
<td>60%</td>
</tr>
</tbody>
</table>

It is important that the organisation does not employ a grey hat hacker (whose intentions might be questionable, as discussed in sections 3.3.7 and 6.6). One respondent chose not to answer this question and no further clarifying comments were provided by the individuals responsible for IT. Only 40% of respondents indicated that they apply unique recruitment practices when appointing ethical hackers. This could be an indication that only some of the banks employ ethical hackers internally – or, alternatively, that they prefer to use third party ethical hacking services. It might also be an indication that respondents have perhaps not applied enough thought to the integrity and skills level of ethical hackers employed. They might unknowingly have employed a grey hat hacker.

9.3.9 The experience and qualifications of the individuals responsible for IT

9.3.9.1 Objective of the question

The objective of the ninth question was to determine the experience and qualifications of the individuals responsible for IT, as an indication of their skills and knowledge level (Question 9).

9.3.9.2 Findings and deductions

Table 9.34 The highest qualification of the individuals responsible for IT (own calculation from the questionnaires of individuals responsible for IT) (n=11)

<table>
<thead>
<tr>
<th>Type of qualification</th>
<th>Count</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>B degree to a D degree.</td>
<td>3</td>
<td>27%</td>
</tr>
<tr>
<td>Other business-related degrees (such as MBA).</td>
<td>4</td>
<td>36%</td>
</tr>
<tr>
<td>IT qualification.</td>
<td>1</td>
<td>9%</td>
</tr>
<tr>
<td>CA(SA) or similar.</td>
<td>3</td>
<td>27%</td>
</tr>
</tbody>
</table>

Generally, the individuals responsible for IT are well qualified. The type of qualification is mostly business-related, which would be expected, in particular for those employed by
bigger banking institutions.

Table 9.35 The highest IT qualification of the individuals responsible for IT (own calculation from the questionnaires of individuals responsible for IT) (n=11)

<table>
<thead>
<tr>
<th>Type of qualification</th>
<th>Count</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>B degree to a D degree.</td>
<td>1</td>
<td>9%</td>
</tr>
<tr>
<td>IT qualification.</td>
<td>4</td>
<td>36%</td>
</tr>
<tr>
<td>Other (such as certifications, etc.).</td>
<td>2</td>
<td>18%</td>
</tr>
<tr>
<td>None.</td>
<td>4</td>
<td>36%</td>
</tr>
</tbody>
</table>

Although the respondents are well qualified in general, they are not necessarily qualified from an IT perspective. Only one respondent indicated that he had a master’s degree in IT. Four out of the 11 respondents (36%) did not have any kind of IT qualification.

In terms of the number of years of IT governance experience, the experience ranges from 3 to 25 years, with an average of 12 years of IT governance experience among respondents. This implies that respondents obtained their IT knowledge and experience mostly through on-the-job training.

9.3.10 Conclusion

The inclusion of IT governance in King III has highlighted the growing importance of IT in business today. King III recommends that the CEO appoints a CIO to manage the IT function and help fulfil the organisation’s IT governance objectives. Irrespective of the size of the bank, it will rely significantly on IT systems and should have an individual responsible for the management of IT.

The results of the questionnaires have highlighted that most individuals responsible for IT are satisfied with the support they received from the board of directors. These individuals were satisfied with the board of directors’ response to IT risk, cybercrime and hacking. Nonetheless, the IT skills level of some board members was questioned by at least half of the respondents. Although the individuals responsible for IT were of the opinion that their IT governance practice compared favourably with their competitors, this was not necessarily reflected in the disclosure of IT governance practices in the annual results of banks, and neither was an indication of which method they would apply given. The individuals responsible for IT were more confident in their organisation’s ability to deal with IT risks and challenges. IT governance has been recognised as key in fighting cybercrime. Achieving business objectives or strategy has been seen as key to incorporating IT governance into
the organisation. Similar to the company secretaries, the individuals responsible for IT did not understand the link between physical risk and IT risk, and the likelihood of physical attacks by hackers. The link between human resource risk and IT risk has also scored low, considering the significance of the insider threat. It is also not well understood how the moral viewpoints of hackers require a different and more targeted response, despite the growing threat of hactivism internationally.

The questionnaire has highlighted that the individuals responsible for IT recognise hacking as a significant threat to the organisation, although it does not appear on the board of directors’ agenda. The effect of hacking on the IT risks, physical access risk and lack of software development were not well understood by the individuals responsible for IT. This is surprising considering that poor software development practices typically introduce software vulnerabilities, which may be exploited by hackers. Technical responses are considered the most effective type of response to hacker attacks, while most individuals responsible for IT were not as confident in employee vigilance as a response. Criminal awareness of the success of hacking has been seen as the most significant factor which increases hacking in the banking sector.

The individuals responsible for IT indicated in the questionnaires that information security management and security technologies are top responses to hacking. Again, despite the fact that ethical hacking is regarded as an effective response to the threat of hacking, the individuals responsible for IT have ranked it as the third last most effective response against hacking, followed by governance frameworks in last position, despite the fact that governance frameworks such as CobiT have been specifically highlighted in King III. The individuals responsible for IT also do not realise that security technologies do not provide a comprehensive response to the threat of hacking.

The questionnaire highlighted that the individuals responsible for IT do recognise the importance of the ethical hacking response in the banking sector and that most have used ethical hacking at some point. The skills level of the ethical hacker is regarded as paramount in the success of an ethical hacking assignment. Most individuals responsible for IT agree that ethical hacking is used to identify and remediate information security and software vulnerabilities. Unique recruitment practices when appointing ethical hackers have only been followed by some banks.
9.4 COMPARATIVE FINDINGS

A few similar questions were included in both surveys, in order to compare the responses between the company secretaries and the individuals responsible for IT. This reflects on the differences in perspective there might be between the company secretaries and the individuals responsible for IT on matters such as IT governance, business risk, IT risk and hacking. Similarly, some of the findings from the analysis of the annual reports (section 7.5) can also be included here and compared to the responses by the company secretaries and the individuals responsible for IT.

9.4.1 Comparative views on the board and IT governance

The first comparison that will be presented, is the views on the board on IT governance from the two questionnaires. In the table below, the weighted arithmetic mean results, reflected as a percentage of the highest possible weighted arithmetic mean from each table is compared.

Table 9.36 Comparative views on the board and IT governance (own calculation from Tables 9.2 and 9.19)

<table>
<thead>
<tr>
<th>Views on the board and IT governance</th>
<th>Highest possible weighted arithmetic mean %</th>
</tr>
</thead>
<tbody>
<tr>
<td>The board of directors takes responsibility for IT governance.</td>
<td>88%</td>
</tr>
<tr>
<td>The board of directors effectively addresses IT governance.</td>
<td>78%</td>
</tr>
<tr>
<td>The board members have the necessary skills to deal with IT matters.</td>
<td>84%</td>
</tr>
<tr>
<td>IT governance is a key component of corporate governance in our organisation.</td>
<td>63%</td>
</tr>
<tr>
<td>IT governance is high on the board’s agenda.</td>
<td>75%</td>
</tr>
<tr>
<td>Our IT governance practices compare favourably with those of our competitors.</td>
<td>60%</td>
</tr>
<tr>
<td>The board’s overall response to IT risk is good.</td>
<td>80%</td>
</tr>
<tr>
<td>The board’s overall response to cybercrime is good.</td>
<td>64%</td>
</tr>
<tr>
<td>The board’s overall response to hacking is good.</td>
<td>83%</td>
</tr>
</tbody>
</table>

The individuals responsible for IT were generally more conservative in their rating of IT governance and the board. In particular, the individuals responsible for IT have rated the board’s overall response to IT risk, cybercrime and hacking lower than the company secretaries did. This indicates that the individuals responsible for IT believe the board of directors can do more to address these threats. Both the company secretaries and the individuals responsible for IT were concerned about the skills level of the board of directors (the highest standard deviation values in Table 9.36). The individuals responsible for IT were
not as convinced as the company secretaries that IT governance is high on the board of directors’ agenda.

9.4.2 Comparative views on IT in their business

The next comparison to consider is the views on IT in business from the two questionnaires. Again the weighted arithmetic means as a percentage is presented.

Table 9.37 Comparative views on IT in business (own calculation from Tables 9.3 and 9.20)

<table>
<thead>
<tr>
<th>The views on IT in business</th>
<th>Highest possible weighted arithmetic mean %</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Company Secretary</td>
</tr>
<tr>
<td>Our ability to deal with IT challenges is good.</td>
<td>83%</td>
</tr>
<tr>
<td>Our ability to deal with IT risk is good.</td>
<td>83%</td>
</tr>
<tr>
<td>IT plays a key enabling role in our products and services.</td>
<td>93%</td>
</tr>
<tr>
<td>Our IT governance practices are key to fighting cybercrime.</td>
<td>85%</td>
</tr>
</tbody>
</table>

Again, the individuals responsible for IT had a slightly more conservative opinion regarding the organisations’ ability to deal with IT challenges and risk than the company secretaries did. It is surprising that the individuals responsible for IT did not rate the organisation’s dependency on IT as higher.

9.4.3 Comparative views on incorporating IT governance into the organisation

As to the views on why IT governance should be incorporated into the organisation, the comparison (the rankings and the weighted arithmetic means as a percentage are presented) between the two questionnaires highlighted the following.

Table 9.38 Comparative views on incorporating IT governance into the organisation (own calculation from Tables 9.4 and 9.21)

<table>
<thead>
<tr>
<th>Views on incorporating IT governance into the organisation</th>
<th>Company Secretary</th>
<th>Individual responsible for IT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Ranking</td>
<td>Highest possible weighted arithmetic mean %</td>
</tr>
<tr>
<td>Regulatory requirements or legislation.</td>
<td>1^st</td>
<td>77%</td>
</tr>
<tr>
<td>Achieving business objectives or strategy.</td>
<td>2^nd</td>
<td>73%</td>
</tr>
<tr>
<td>Growth in complexity of the IT function.</td>
<td>3^rd</td>
<td>68%</td>
</tr>
<tr>
<td>Industry norm and practice.</td>
<td>4^th</td>
<td>45%</td>
</tr>
<tr>
<td>The culture of the organisation.</td>
<td>5^th</td>
<td>45%</td>
</tr>
</tbody>
</table>
The views of the company secretary and the individual responsible for IT regarding the reasons for the incorporation of IT governance into the organisation were very similar, from a ranking perspective.

### 9.4.4 Comparative views on the links between business risk and IT risk

The weighted arithmetic mean scores as a percentage, from the questionnaires to both the company secretaries and individuals responsible for IT, regarding the link between various business risks and IT risk are reflected in Table 9.39.

<table>
<thead>
<tr>
<th>Views on the links between business risk and IT risk</th>
<th>Highest possible weighted arithmetic mean %</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Company Secretary</td>
</tr>
<tr>
<td>Technology risk.</td>
<td>93%</td>
</tr>
<tr>
<td>Business continuity risk.</td>
<td>90%</td>
</tr>
<tr>
<td>Disaster recovery risk.</td>
<td>90%</td>
</tr>
<tr>
<td>Operational risk.</td>
<td>88%</td>
</tr>
<tr>
<td>Reputational risk.</td>
<td>82%</td>
</tr>
<tr>
<td>Compliance risk.</td>
<td>77%</td>
</tr>
<tr>
<td>Credit risk.</td>
<td>77%</td>
</tr>
<tr>
<td>Market risk.</td>
<td>75%</td>
</tr>
<tr>
<td>Human resource risk.</td>
<td>73%</td>
</tr>
<tr>
<td>Physical risk.</td>
<td>63%</td>
</tr>
</tbody>
</table>

The ranking of the responses between the company secretaries and the individuals responsible for IT are very similar. This implies that the two groups hold similar views on business risks and how they are affected by IT risk. This may also highlight certain shared misconceptions about IT risk and how it affects business risk, which may catch the banking sector off-guard. An example here is the misconception that there is not a strong link between physical risk and IT risk. This is clearly an area of weakness hackers may take advantage of. Technology risk, disaster recovery risk, human resource risk and physical risk were disclosed in only a few annual reports (Table 7.6), in contrast to the relative importance given to those risks by the company secretaries and individuals responsible for IT.

### 9.4.5 Comparative views on hacking and IT risk

In Table 9.40 comparative views (the weighted arithmetic means as a percentage) between the questionnaires, regarding the extent to which hacking will increase IT risks is provided.
Again, the ranking of the responses between the company secretaries and the individuals responsible for IT are very similar.

<table>
<thead>
<tr>
<th>The extent to which hacking will increase IT risk</th>
<th>Highest possible weighted arithmetic mean %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybercrime.</td>
<td>95%</td>
</tr>
<tr>
<td>Logical access risk.</td>
<td>92%</td>
</tr>
<tr>
<td>IT systems risk.</td>
<td>90%</td>
</tr>
<tr>
<td>IT continuity risk.</td>
<td>88%</td>
</tr>
<tr>
<td>Communications failure.</td>
<td>87%</td>
</tr>
<tr>
<td>IT non-compliance risk.</td>
<td>82%</td>
</tr>
<tr>
<td>Physical access risk.</td>
<td>80%</td>
</tr>
<tr>
<td>IT human resources risk.</td>
<td>70%</td>
</tr>
<tr>
<td>Lack of software development.</td>
<td>63%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Company Secretary</th>
<th>Individual responsible for IT</th>
</tr>
</thead>
<tbody>
<tr>
<td>95%</td>
<td>89%</td>
</tr>
<tr>
<td>92%</td>
<td>93%</td>
</tr>
<tr>
<td>90%</td>
<td>84%</td>
</tr>
<tr>
<td>88%</td>
<td>91%</td>
</tr>
<tr>
<td>87%</td>
<td>73%</td>
</tr>
<tr>
<td>82%</td>
<td>80%</td>
</tr>
<tr>
<td>80%</td>
<td>75%</td>
</tr>
<tr>
<td>70%</td>
<td>77%</td>
</tr>
<tr>
<td>63%</td>
<td>63%</td>
</tr>
</tbody>
</table>

The results illustrate that there is a common understanding of IT risks and how these may be affected by hacking between the two groups. But, this common understanding could be a common misconception. For example, the lack of software development has been ranked last. Poor software development practices are the root cause of software vulnerabilities (discussed in section 3.8.5). This is specifically targeted by hackers. Consequently, this has been ranked too low by both groups of respondents. Generally, with the exception of IT continuity risk, IT risk themes have not been disclosed in the annual results (Table 7.7). There is clearly a gap in terms of the significance of these IT risks in practice versus disclosure of these risks in the annual reports.

### 9.4.6 Comparative views on general responses to hacking

As to the responses to the risk of hacking, comparative views (the weighted arithmetic mean results, reflected as a percentage of the highest possible weighted arithmetic mean from each table is compared) between the results of the questionnaires are provided in Table 9.41.

The individuals responsible for IT were slightly more optimistic than the company secretaries regarding security technologies and information security management as a response to hacking in most cases. There was general agreement between the company secretaries and the individuals responsible for IT regarding the ranking of the top five responses to hacking. Only some of the responses are disclosed by several of the banks in their annual reports.
(Table 7.8), such as information security management, IT governance, risk management and corporate governance.

Table 9.41 Comparative views on the responses to the risk of hacking (own calculation from Tables 9.15 and 9.27)

<table>
<thead>
<tr>
<th>Responses to the risk of hacking</th>
<th>Company Secretary</th>
<th>Individual responsible for IT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security technologies, such as firewalls.</td>
<td>88%</td>
<td>95%</td>
</tr>
<tr>
<td>Information security management.</td>
<td>86%</td>
<td>96%</td>
</tr>
<tr>
<td>Internal control.</td>
<td>85%</td>
<td>85%</td>
</tr>
<tr>
<td>IT governance.</td>
<td>85%</td>
<td>89%</td>
</tr>
<tr>
<td>Risk management.</td>
<td>83%</td>
<td>85%</td>
</tr>
<tr>
<td>Software development practices.</td>
<td>79%</td>
<td>75%</td>
</tr>
<tr>
<td>Corporate governance.</td>
<td>72%</td>
<td>69%</td>
</tr>
<tr>
<td>Ethical hacking.</td>
<td>68%</td>
<td>73%</td>
</tr>
<tr>
<td>Governance frameworks, such as CobiT.</td>
<td>68%</td>
<td>75%</td>
</tr>
<tr>
<td>Applying service and quality management, such as ITIL.</td>
<td>64%</td>
<td>78%</td>
</tr>
</tbody>
</table>

Other responses have not been reported in line with the relevant importance afforded to those responses by the company secretaries and individuals responsible for IT. This could either point to a lack of disclosure of some responses in the annual reports, or indicate the reality of the specific bank not making use of a particular response to IT risk or hacking.

Table 9.42 Comparative views on the effectiveness of the general responses to the risk of hacking (own calculation from Tables 9.16 and 9.28)

<table>
<thead>
<tr>
<th>The effectiveness of general responses to the risk of hacking</th>
<th>Company Secretary</th>
<th>Individual responsible for IT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security technologies, such as firewalls.</td>
<td>81%</td>
<td>93%</td>
</tr>
<tr>
<td>Information security management.</td>
<td>77%</td>
<td>89%</td>
</tr>
<tr>
<td>Internal control.</td>
<td>76%</td>
<td>80%</td>
</tr>
<tr>
<td>IT governance.</td>
<td>75%</td>
<td>76%</td>
</tr>
<tr>
<td>Risk management.</td>
<td>73%</td>
<td>78%</td>
</tr>
<tr>
<td>Software development practices.</td>
<td>71%</td>
<td>73%</td>
</tr>
<tr>
<td>Corporate governance.</td>
<td>67%</td>
<td>75%</td>
</tr>
<tr>
<td>Ethical hacking.</td>
<td>60%</td>
<td>71%</td>
</tr>
<tr>
<td>Governance frameworks, such as CobiT.</td>
<td>60%</td>
<td>65%</td>
</tr>
<tr>
<td>Applying service and quality management, such as ITIL.</td>
<td>59%</td>
<td>69%</td>
</tr>
</tbody>
</table>

The results presented in Table 9.42 are very similar to those in Table 9.41. Respondents in general rated the effectiveness of a response close to the use of the response. This could indicate that the nature of the response might lend itself to a certain perception of level of effectiveness. It is clear that ethical hacking is not used to its fullest potential, seeing that it has been ranked lower than responses that are less effective than ethical hacking. But
based on the extensive literature review performed in this study (as indicated in Table 6.5), this perception among company secretaries and individuals responsible for IT is wrong.

9.4.7 Conclusion

In general, comparative results between the company secretaries and individuals responsible for IT were similar. The ratings of the individuals responsible for IT were lower for the board of directors’ responsibility for IT governance, than the ratings of the company secretaries. In particular, the individuals responsible for IT rated the board’s overall response to IT risk, cybercrime and hacking lower than the company secretaries. The company secretaries and individuals responsible for IT alike were concerned about the IT skills level of the board of directors.

There is a common misconception among the company secretaries and individuals responsible for IT regarding the extent of the link between business risks (such as human resource risk and physical risk) and IT risk. The responses of the company secretaries and individuals responsible for IT did not match the results of the annual report disclosures. This indicates a lack of disclosure of the business risks, IT risks themes and responses to hacking identified in this thesis.

9.5 FINAL OUTCOME OF THE RESEARCH OBJECTIVES AND RECOMMENDATIONS

This section contains the outcome of both the literature review and the results from the questionnaires, outlined against each of the primary research objectives defined in section 1.4.

9.5.1 Given that hackers often target banks, determine what the responses to hacking are in the South African banking sector

9.5.1.1 Deductions from the research findings

The literature review has highlighted that the board of directors needs to ensure that it has the required skills in place to face challenges posed by technology. As part of their corporate governance responsibilities, risk management should be applied to manage pervasive risks, such as IT risk (section 5.3.1). According to the views of the company secretaries, the board
of directors’ overall response to cybercrime and hacking is good, despite the fact that company secretaries and the individuals responsible for IT highlighted that the board of directors does not have the necessary skills to deal with IT matters.

This study has highlighted that IT governance seeks to achieve a balance between the risks and benefits derived from IT. Effective IT governance practices will address the business risks associated with IT (section 5.6.1). The company secretaries and the individuals responsible for IT indicated that IT governance practices are only used to some extent to fight cybercrime. Exactly how IT governance can be used as a response might be unclear to the company secretaries. This study has identified insider attacks as a significant threat to organisations today (section 3.5.3.6). The individuals responsible for IT indicated that their organisations’ response to insider attacks is not as effective as it should be.

The literature review highlighted the various underlying motives of hackers, which could be a strong driving force behind their attacks (section 3.5.2). Some hackers can also be classified as hacktivists, and perpetrate their crimes on the basis of a particular moral point of view (section 3.5.3.2). Most of the individuals responsible for IT were also not aware that the moral viewpoint of hackers will affect the response required to hacker attacks. The awareness regarding hackers being driven by their moral viewpoint is very low, which is surprising given the fact that there is a growing trend of hacktivism which is well publicised in the media. The risk of hacktivist attacks may therefore be underestimated.

The primary responses to the risk of hacking in the South African banking sector from the perspective of the company secretaries and individuals responsible for IT include security technologies, information security management and IT governance. These all cover detective and preventative controls that could be used to respond to hacking. However, as has been argued in this thesis, none of these fully address the risk of hacking (section 5.10 and Table 5.5). Respondents also agree that technical responses are “good”, but not perfect. It has to be emphasised that technical responses in the form of security technologies only provide partial coverage of the IT risk themes identified in this thesis (Table 5.4).

Hackers at times make use of non-technical attack techniques, commonly referred to as social engineering (section 3.9.4). These can be just as effective as technical attack techniques. This kind of attack can be detected only by being vigilant and observant about unusual activities. Employee vigilance, however, was not rated very high by the individuals responsible for IT as an effective response to hacker attacks, and this indicates that social engineering attacks have a strong likelihood of succeeding at some banks.
Software development practices could contribute significantly to decreasing software vulnerabilities (section 5.8.2). Software development practices were rated low by the individuals responsible for IT, considering that secure software development practices could help prevent the exploitation of vulnerable software by hackers.

Ethical hacking has been identified in this thesis as the most comprehensive response to hacking (Table 6.5). Ethical hacking is used by most banks as a response, although it was ranked in eighth position by the company secretaries and in ninth position by the individuals responsible for IT. It is clear that the company secretaries and the individuals responsible for IT do not recognise the comprehensive nature of ethical hacking as a response. Although not as comprehensive as ethical hacking, CobiT has been identified as one of the more comprehensive responses to IT risk (Table 6.5). A governance framework such as CobiT was also ranked low by the company secretaries, despite being listed in King III. It indicates that governance frameworks are not extensively used as a response to hacking.

In terms of the effectiveness of the responses to hacking, the company secretaries and the individuals responsible for IT highlighted security technologies, information security management, and internal control as the most effective responses to hacking. This study has argued that these are not the most comprehensive responses to IT risk and hacking (Table 6.5). The company secretaries and the individuals responsible for IT might therefore have a false sense of security. Software development was rated sixth by the company secretaries and seventh by the individuals responsible for IT in terms of the effectiveness of the response. This ranking suggests that secure software development practices are effectively applied at only some banks as a response to hacking.

There are many advantages associated with ethical hacking, including finding vulnerabilities and strengthening the organisation’s defences against hacker attacks (section 6.10). Ethical hacking has been used by most banks at some point. Ethical hacking was rated as the eighth effective response by the company secretaries and the individuals responsible for IT respectively. Only some individuals responsible for IT saw ethical hacking as advantageous to identifying and remediating information security and software vulnerabilities. This indicates that ethical hacking has not yet been commonly accepted as an effective response to hacking in the banking sector and that the banking sector may be at risk of being successfully attacked by hackers if they are not using the most effective response to hacking.

The various skills requirements for ethical hackers were identified in the literature study
The results of the questionnaires indicate that the skills level of ethical hackers are considered a determining factor in the success of ethical hacking assignments, and indicate that ethical hacking is either applied incorrectly or the required skills level of ethical hackers used by the banking sector is not on par with the expectations of the individuals responsible for IT. Governance frameworks were also rated low in terms of effectiveness, which indicates that they are not applied effectively as a response to IT risk and hacking.

This study has highlighted the risk of hackers circumventing physical access by targeting mobile computing devices (section 3.8.3.2). There is some awareness among respondents that hacking as a risk is moving from traditional platforms, such as PCs in general, to mobile devices.

9.5.1.2 Recommendations

The company secretaries and individuals responsible for IT are of the opinion that responses such as information security management and security technologies are the best responses to the risk of hacking. More consideration should be given to the most effective responses to IT risk and hacking, such as internal control, governance frameworks such as CobiT and ethical hacking. The effectiveness of ethical hacking as a response needs to be recognised in the context of other responses. More attention needs to be given to the evolving nature of hacking. In particular, the growing threat of hactivism and the determined nature of these individuals need to be recognised, to ensure the appropriate response. Ethical hacking should be carried out in all its facets, as a significant response to the risk of hacking. In particular, emphasis should be placed on the use of ethical hacking during software development. Consideration should also be given to the appropriate response to the physical risk associated with hackers. Ethical hacking can be used to test the effectives of physical controls, not only technical controls. More importantly, ethical hacking as a response needs to be elevated to a corporate governance level, to ensure that the board of directors understands the concept and insists on and enquires about the use of ethical hacking.

9.5.2 Determine what the depth of the governance responses to hacking is in the local banking sector

9.5.2.1 Deductions from the research findings

The board of directors has a role to play in the governance responses to hacking. For example, it has to ensure that appropriate information security management practices have been considered in carrying out their IT responsibilities (section 5.2). The threat of hacking
or cybercrime can be dealt with via the IT governance responsibilities of the board of directors (identified as role-players in the IT governance response in section 5.6.4). Considering that not all the boards of directors have fully accepted their IT governance responsibilities (as indicated by the varied responses from the individuals responsible for IT), the response to hacking may not be dealt with by the board of directors. Moreover, there may be several factors which contribute to the board of directors' inability to deal with these IT matters. The overall responsibility for IT has been assigned to a particular board member at only five banks. Both the company secretary and the individual responsible for IT have highlighted the lack of IT skills to deal with IT governance. Furthermore, IT matters discussed at other committees may not reach the board of directors at some banks, as meeting minutes containing IT matters may not reach the board of directors. Hacking is on the board of directors' agenda only at a few banks. The company secretaries rated the effectiveness of the corporate governance response to the risk of hacking in seventh position and IT governance in fourth position. The individuals responsible for IT rated the effectiveness of the corporate governance response in sixth position and IT governance in fifth position. The individuals responsible for IT and the company secretaries are therefore unclear as to how these responses can be effectively applied as a response to hacking.

Security technologies, information security management, internal control and risk management have been highlighted as the most effective responses to hacking. Other response types have been rated lower, although not considerably lower. Security technologies and information security management were considered the most effective responses by the individuals responsible for IT. The literature review has shown, however, that these responses are not the most effective responses to the threat of hacking (Table 5.5). Governance responses such as CobiT have also been rated very low by both the company secretaries and the individuals responsible for IT. The lack of governance responses indicates that the board of directors has not yet taken full ownership of IT governance.

This study has established that ethical hacking can be applied as a complete approach to information security or as part of a larger information security strategy (section 6.9.1). The questionnaires have highlighted that ethical hacking is used as a response by most banks, although not as extensively as other governance responses. The effectiveness of the ethical hacking response is not fully recognised in the banking sector.
9.5.2.2 Recommendations

There are certain misconceptions in the banking sector as to the effectiveness of some of the traditional responses to hacking. It is strongly recommended that these deficiencies are addressed by applying ethical hacking to augment the traditional responses to hacking. The extent to which ethical hacking is applied is also not adequate.

IT governance should be elevated to a board of directors level, similar to the importance of the audit committees or risk committees at board level. This can be achieved by establishing an IT committee at board of directors’ level. Alternatively, the responsibility for IT should be allocated to a particular board member. A range of IT matters (including hacking) should be included in the agenda of the board. Meeting minutes of other committees dealing with IT matters should be included in the board packs. Only then will IT receive appropriate attention as a business enabler. Governance responses, such as CobiT, should also be considered as a response to hacking. Although it is not the most comprehensive response, it provides significantly better coverage of IT risks than security technologies. It will also enable closer integration with corporate governance and facilitate the formation of IT governance practices.

Ethical hacking as a concept is still not fully understood in the banking sector. Therefore, clear guidance and education is required in the banking sector to highlight the effectiveness of ethical hacking as a response. Ethical hacking has also not been promoted at a governance level. The board of directors needs to be made aware of the benefits associated with ethical hacking. The company secretary can play a role in including IT training in the board of directors’ programme of work for the year. This could include an overview of the nature of ethical hacking as a response.

9.5.3 Established whether the board of directors provide sufficient oversight and focus on IT risk in the local banking sector

9.5.3.1 Deductions from the research findings

It has been established in the literature review that the board of directors carries the ultimate responsibility for risk management in an organisation (section 5.3.1).

The company secretaries and individuals responsible for IT held varied opinions as to the board of directors’ focus and oversight on IT risks. The individuals responsible for IT were
not as satisfied as the company secretaries with the board of directors’ IT risk oversight role. A possible root cause for this is the lack of IT skills at board of director level. Although IT matters are routinely added to the agenda of the board of directors, the depth of discussion of these IT matters is unclear. Detailed discussions of IT risk could be delegated to other committees such as risk management or IT steering committees. IT risk is perhaps not yet treated equally to other business risks. In terms of the different IT risk themes (identified in Table 4.30), not all were considered significant by the company secretaries or the individuals responsible for IT, although all can be affected by hacking.

Most of the IT risk themes identified in this thesis were not disclosed in the annual reports of the banks (Table 7.7). This also indicates that IT risk is not given enough priority in the banking sector.

9.5.3.2 Recommendations

Greater focus is required on the impact of IT risk on business risk. The concept IT risk is complex and education is required in the banking sector, in particular at a board of director level, to ensure that greater awareness exists around the IT risks themes identified in this thesis. Again, the company secretary can play a role in scheduling appropriate training sessions on IT matters. In addition, greater awareness is required regarding how IT risk affects the various business risks. This increased awareness will lead to an increased focus on IT risk. The increased focus can be accomplished by appointing members of the board with sufficient IT skills to lead the discussions on IT risk. The responsibility for IT matters could also be delegated to a particular board member, who could attend other committees where IT matters are discussed. Or IT matters could be delegated to a board level IT steering committee.

Also, increased disclosure of the IT risk themes identified in this thesis is required. It should be clear from annual reports whether banks are adequately mitigating IT risk. This includes disclosure of the responses to IT risk, including hacking.
9.5.4 Determine whether hacking is considered a threat in the local banking sector

9.5.4.1 Deductions from the research findings

This study has provided an extensive discussion of the effects of hacking on business (sections 3.12 and 3.13). The individuals responsible for IT were less satisfied than the company secretaries with the board of directors’ overall response to cybercrime and hacking. This indicates that the individuals responsible for IT believe the board of directors should pay closer attention to cybercrime and hacking. The company secretaries were of the opinion that IT governance practices are only used to some extent to fight cybercrime. The reliance placed on security technologies as a response to hacking indicates that the response to hacking could be more of a tactical response than a governance response. The board of directors is not fully participating in the response to hacking and cybercrime.

The company secretaries and the individuals responsible for IT agreed on the strong link between technology risk and business risk. Inherently, IT risk is a component of technology risk (section 4.3.5.4), and in turn hacking is a component of IT risk (section 4.4.1). As argued in this thesis, hacking is strongly linked to business risk (Table 4.32). This intrinsic link is perhaps not clearly understood by the company secretaries and individuals responsible for IT. The company secretaries and the individuals responsible for IT agreed on hacking strongly increasing the IT risk of cybercrime. Hacking is also intrinsically part of cybercrime (section 3.10). However, given the low ranking of other IT risks, such as physical access risk, IT human resource risk and lack of software development, the company secretaries and the individuals responsible for IT do not fully comprehend yet how hacking can be a threat to other IT risk themes.

Most individuals responsible for IT regarded hacking as a significant threat in their respective organisations, and not simply a perceived risk. What is of concern is that 36% of the individuals responsible for IT did not believe hacking is a significant threat. This implies that the risk of hacking is underestimated at some banks. According to the literature study, a strong link exists between hacking, IT risk and reputational risk (section 4.12). Most individuals responsible for IT agreed that hacking could significantly increase an organisation’s reputational risk. Most individuals responsible for IT agreed that hacking should be detected. Fewer agreed that it should be prevented, which again highlights that some banks might be at risk of hacking attacks.
The findings of the literature review indicated that hacking is generally associated with criminal activity today, as established in this thesis (section 3.2.3). The individuals responsible for IT were aware of the increase of criminal awareness among hackers. There is therefore general awareness in the banking sector of this growing threat. The responses to hacking suggest that hacking is definitely not a new threat. The use of security technologies such as firewalls implies a tactical response and daily on-going protection against hacker attacks. The individuals responsible for IT have also given a very mixed response in terms of the risk of internal insider attacks versus external hacker attacks. The risk of an insider attack is definitely underestimated, which is suggested by less focus being placed on physical risk and human resource risk than other business risks. In addition, given that the individuals responsible for IT did not clearly understand how a hacker’s motives could increase hacker attacks, the motivations of hackers are also not understood. The risk of hacktivism is therefore underestimated.

9.5.4.2 Recommendations

Greater awareness of the threat of insiders, hacktivism and hacker attacks via social engineering techniques on the physical premises of an organisation needs to be created, to ensure that the banking sector can respond appropriately. The company secretary could play a role in ensuring that these issues are included in IT training workshops for the board of directors. Guidelines on these threats can also be published in the banking sector. Established organisations which already provide awareness around cybercrime issues, such as Sabric, could take ownership of awareness campaigns and publications. Greater transparency from the banking sector is required in terms of the number of significant hacker attacks against banks.

9.5.5 Determine the extent to which banks make use of ethical hacking as a possible response to the threat of hacking

9.5.5.1 Deductions from the research findings

Ethical hacking has been identified in this thesis as the most comprehensive response to hacking (Table 6.5). Most banks have indicated that they have made use of ethical hacking at some point. However, the responses to the use and effectiveness of the various responses to hacking indicate that ethical hacking is not used as a primary response to the threat of hacking. Ethical hacking has been regarded as an effective response to hacking in general, but this is not reflected in the ranking given to ethical hacking by respondents in this
study. Ethical hacking is perhaps used instead on an ad hoc basis. Furthermore, only a few individuals responsible for IT have indicated that they make use of special recruitment practices, which indicates that banks may be making use of third-party ethical hacking services instead (discussed in section 6.6). This further supports the notion of the ad hoc use of ethical hacking in the banking sector.

Several disadvantages associated with ethical hacking have been identified in this thesis (section 6.11). The individuals responsible for IT were not overly concerned about the disadvantages associated with ethical hacking, however. They clearly understood that ethical hacking can be used to identify security vulnerabilities and test internal control against hacker attacks. Most banks were of the opinion that human resources risk and physical risk are not affected by IT risk, and these are potential areas of weakness which could be tested using ethical hacking. This will highlight any potential weaknesses that may be exploited by hackers in these risk areas.

This study has argued that ethical hacking can be applied as part of software development to enhance application security (section 6.9.2). The questionnaires have highlighted that not enough focus is given to software development practices, which is often the point of origin for software vulnerabilities that can be exploited by hackers. Again, ethical hacking can be used extensively during software development to reduce software vulnerabilities significantly (as highlighted in section 6.9.2).

9.5.5.2 Recommendations

Given the comprehensiveness of ethical hacking as a response to the threat of hacking, as argued in this thesis, the banking sector could increase the use of ethical hacking. Ethical hacking needs to be recognised as a governance response to the threat of hacking by the company secretaries, the individuals responsible for IT and the board of directors. The individual responsible for IT could be the champion of ethical hacking, which should not be performed in isolated cases. Ethical hacking needs to be recognised as a response with multiple areas of application. The skill and insight of ethical hackers need to be acknowledged in the banking sector. Ethical hacking should be used extensively to identify security and software vulnerabilities. The use of software development frameworks such as OWASP, SAMM and MSDL should also be encouraged. Recruitment guidelines for ethical hackers can be made available to the banking sector.
9.6 CHAPTER SUMMARY

This chapter presented the results of the empirical fieldwork. These results support the use of IT governance practices in the banking sector, although not necessarily at board of directors’ level. IT risk does not feature prominently yet at board of directors’ level. Some IT risks might be neglected or the impact of hacking on those IT risks could be underestimated. This poses a real threat to the banking sector at large.

There is a misconception in the banking sector about the effectiveness of governance responses to hacking, such as information security management and security technologies. Ethical hacking does not have the prominence of other responses to hacking in the banking sector. The banking sector could therefore benefit greatly from increasing its use of ethical hacking to protect itself against this growing threat.
10.1 INTRODUCTION

This chapter provides final conclusions based on the literature review and the questionnaires. Some of the key findings of this study are underscored. Final recommendations are presented and areas for further research are highlighted.

10.2 CONCLUSIONS

10.2.1 Conclusions from the literature study

The literature study has clearly highlighted the stark reality of the hacking threat to business today. Organisations are critically dependent on technology for their daily operations, and to remain competitive in an ever-expanding world organisations not only have to embrace new technology. They also have to face the threats that evolve from the same technology they so acutely depend on.

The most significant findings from the literature study have been summarised against each of the overarching objectives defined in section 1.4.

1. **Outline how IT has affected business from a historical perspective, which eventually led to the introduction of IT governance.**

   IT has become an enabler for business and increasingly reliance is placed on IT to support business growth, and to provide control and critical management information. At the same time, IT also introduces significant risk. It has become imperative for organisations to balance the benefits derived from IT with the risks associated with IT.

   Increased focus on the proper functioning and integration of IT with business, towards achieving the organisation’s strategic objectives, is required. This has introduced IT governance, which places the responsibility for IT on the board of directors’ agenda. IT governance introduces structure and control over IT resources and ensures that those
IT resources support the achievement of organisational objectives.

The board of directors is not only responsible for the effective utilisation of IT resources. It is also responsible for managing the risks associated with IT. This has become part of its fiduciary duties. It has to ensure that the various management disciplines are in place to effectively mitigate IT risk. Therefore IT governance has to be executed in conjunction with other governance disciplines, such as risk management and information security management. The emergence of hacking as a threat and significant IT risk to organisations today requires attention at the highest level of the organisation. The board of directors has to take note of IT risk as a significant business risk, which includes hacking as a risk. The board of directors needs to ensure appropriate responses are implemented to protect the organisation against these threats.

2. Delve into the meaning and nature of hacking, towards understanding the significance of this threat in today’s business world.

Although the hacking phenomenon emerged from the general interest in the inner workings of PCs and writing efficient software programs, it quickly evolved into a more sinister activity, aimed at exploiting computer technology, committing fraud or theft, and other malicious activities.

It has been established from the literature that hacking is now generally regarded as the malicious activity of breaking into organisations’ networks and PCs without authorisation and with the illegal intent of misusing, stealing or blocking IT resources and other assets, such as intellectual property contained in custom-developed systems and electronic funds. A hacking culture has emerged from the 1980s, which is largely still the same today, although it is increasingly involved in organised crime and cybercrime activities. Six different hacker profiles can be distinguished from the literature: script kiddies, crackers, über hackers, black hat hackers, white hat hackers and grey hat hackers. The profiles reveal that hackers differ in two important respects: their skills level, and their ethical and moral viewpoints. Importantly, these variations will lead to different levels of threat to organisations, which requires different levels of response. Hackers acquire their skills mostly online, from other hackers or the vast availability of free resources on the subject.

Hackers have various objectives in their malicious activity, including pursuing
organised crime, engaging in hacktivism for a specific cause, such as gaining unhindered access to information, vigilantism against other criminal offenders on the Internet, industrial espionage and terrorism. It has also been established from the literature that hackers could be inside an organisation, where the potential damage is even greater than that stemming from attacks originating from outside the organisation.

An important consideration for the South African banking sector is the growing threat of hacking in the South African context. South Africa has also become a prominent user of the Internet, with the demand for Internet bandwidth increasing and more organisations creating an online presence. Cybercrime and hacking are increasing in South Africa, with significant losses being reported in the media. Our closer interaction and integration with the global marketplace via the Internet also exposes South Africa to the significant and growing threat of hacking and cybercrime internationally. It is critical to understand how this impacts an organisation's business risk.

3. **Identify common weaknesses found in organisations which facilitate and lead to hacker attacks.**

Hackers follow a general methodology during their attacks, and various hacker tools and technologies have been developed and are available in both free and commercial form to aid hackers in their illegal activity. There are several weaknesses that facilitate successful hacking attempts. Weaknesses associated with physical access, logical access, software and hardware vulnerabilities, and the inherent risk associated with global interconnected networks and human fallibility facilitate and lead to successful hacker attacks.

4. **Provide an overview of the motives and attack techniques of hackers, which may lead to security breaches.**

A wide variety of hacker techniques have also been identified from the literature. These range from non-technical social engineering techniques to advanced technical techniques, taking advantage of software vulnerabilities or the poor configuration of networks, systems and the online websites of organisations. A range of motives drive hackers, such as addiction to computers, social status, curiosity or peer recognition. Hackers have various objectives underpinning their attacks, such as organised crime, hacktivism, vigilantism, terrorism and industrial espionage.
5. **Understand the link between hacking and cybercrime.**

Hacking is a type of cybercrime, and hackers often engage in other cybercrime activities, such as theft of PCs and extortion. There is often collaboration between hackers and other cybercriminals, such as hackers stealing credit card details from an organisation and the cybercriminal selling the credit card details on the Internet.

6. **Provide a critical argument for the classification of the nature of hacking as a risk or as an event.**

One of the most important deductions made from the literature review was to conclude that hacking might be termed an event on the one hand and a risk on the other hand. Hacking can be considered an event that results from a risk or risks that are actively exploited in the present time. The event of hacking would be best reacted upon through detective controls. Hacking can also be considered a risk, where the risk of hacking refers to a future event that will be addressed via preventative controls. The extent to which detective and preventative controls against hacking will be implemented depends on the extent to which hacking is regarded as a threat.

7. **Identify a common list of business risks to facilitate the discussion of the ultimate link between hacking and business risk.**

Although there is no definitive definition of business risk, the risk categories of King II have been used as the foundation of the detailed discussion of business risk and how it is impacted by IT risk. A generic set of IT risk themes have also been identified from a comprehensive literature review. The IT risk themes are also completed by common control objectives. It has further been established that hacking could closely interact with and increase each of the IT risk themes. Considering that there are general links between the IT risk themes and the business risks, it follows that hacking could affect every business risk identified in this thesis.

Physical risk manifests itself from an IT risk perspective, mostly around the protection of physical IT infrastructure. Hackers increase physical risk firstly by gaining unauthorised access to an organisation’s premises and secondly by stealing, damaging or sabotaging IT equipment, systems and networks. Hackers mostly make use of social engineering techniques to gain physical access to an organisation’s premises. Given that an organisation’s network perimeter extends beyond the physical
boundaries of an organisation, hackers make use of techniques such as wardriving to exploit weaknesses in organisations’ networks.

Operational risk consists of people, processes, technology and external factors. The people component relates closely to human resource risk. The technology component relates strongly to IT risk or technology risk. Hackers increase the process component of operational risk by compromising the availability of systems and processes. Poor internal processes, such as weak project management and software development practices, could introduce software vulnerabilities, which are then exploited by hackers. Inefficient IT operations and support could lead to extended periods of downtime. External factors relate to IT risks, such as the lack of compliance with regulatory requirements (for example, the requirement to protect confidential data against hacker attacks).

Human resource risk manifests itself in various forms. Poorly skilled IT resources could introduce weaknesses in the systems and networks that could be exploited by hackers. The critical dependency on key resources could lead to an inability to recover systems after hacker attacks. Disgruntled employees can commit insider attacks, easily compromising system security due to their detailed knowledge of the systems and detective controls. Poor information security practices, such as employees writing down their passwords, could increase the likelihood of hacker attacks. System administrators often ignore the policies and procedures of the organisation, use weak passwords, open systems up to ease the administration burden and consequently introduce significant opportunities for hackers to exploit.

Technology risk and IT risks are closely associated concepts, although the literature review has established that IT risk can generally be regarded as a subset of technology risk. Nineteen common IT risk themes have been identified in this thesis. They all relate directly to technology risk. At the same time, technology risk and IT risk can be increased by hacking, which is fundamentally an IT risk itself.

Business continuity and disaster recovery can be affected by hacking, mostly when hackers compromise system security and destabilise systems and networks in the process. Business continuity and disaster recovery are also closely related to IT risk, with for example failure of internal back-up processes increasing the likelihood of a business recovery scenario. Hackers also often target supporting infrastructure, such as the electrical and telecommunication systems supporting a particular organisation.
Credit risk and market risk could also be affected by hackers in the form of rogue inside traders who compromise system security and execute unauthorised trading activity, which could severely increase the organisation’s market risk and ability to obtain credit in the market. Credit risk and market risk are also intrinsically linked with reputational risk, with a hacking incident impacting the market risk, due to the negative perceptions regarding the organisation’s system security that might exist in the public.

Compliance risk can be increased by hacking, due to the complicated nature of cybercrime legislation and the challenges associated with the prosecution of hackers, who often launch their attacks from other jurisdictions. By their very nature, hackers and insiders ignore the IT policies and procedures of an organisation. Theft of confidential data by hackers could also increase an organisation’s compliance risk, when statutory requirements insist on security precautions for confidential client details.

The literature study has also established that an organisation’s reputational risk can be severely affected by hackers when information about hacking incidents reaches the public, clients or investors. This may result in a loss of confidence in the organisation’s ability to prevent and detect hacker attacks, which in turn increases reputational risk.

8. Identify common IT risk themes and establish the link between hacking and IT risk and control objectives to illustrate that hacking could be the cause of each IT risk theme. Identify a link between hacking, IT risk and a range of business risks identified in this study, to illustrate the intrinsic link between business risk and hacking.

A range of commonly cited business risks have been identified in this thesis from a number of authoritative sources: physical risk, operational risk, human resource risk, technology risk, business continuity and disaster recovery, credit and market risk, compliance risk, and reputational risk. Similarly, a systematic analysis of the literature made it possible to identify 19 IT risk themes, which could be broadly divided into application and general controls. Supplementary to the IT risk themes, eight common control objectives have been identified. In addition to this, an in-depth literature review of hacking revealed various hacking attacks which could affect business. The study mapped each of the business risks against one or more of the IT risk themes. In turn, the various hacking attacks have been mapped against the IT risk themes. The
literature review concluded that there is a strong link between business risks and hacking.

9. **To identify and categorise a range of responses to hacking. Explore the depth of each of the responses to hacking with the purpose of highlighting that none of them are effective enough in addressing all the IT risk themes and by implication the risk of hacking.**

This study has categorised a range of responses to hacking, including corporate governance, risk management, internal control, IT governance, quality management (including software development and project management), service management and information security management. The responses vary in their coverage of the IT risk themes addressed in this thesis, however. Some responses, such as corporate governance, IT governance and risk management, provide only indirect responses to the hacking threat. Other responses, such as IT service management, quality management, project management, software development, and security configuration benchmarks, provide partial or incomplete responses to the threat of hacking. There are however a few responses that provide more comprehensive responses to the threat of hacking.

The literature study showed that the most comprehensive coverage is provided by internal control, the frameworks CobiT 5 and ISO 27002, and security technologies. Internal control provides a very direct response to most of the IT risk themes. The proper functioning of an organisation’s internal control is an essential component in achieving the principles of good corporate governance. The frameworks CobiT 5 and ISO 27002 provide fair coverage of the IT risk themes. Security technologies provide the least coverage of IT risk themes. It is critical to note that none of these responses provide full coverage of the IT risk themes. As a consequence, none of these responses can provide full coverage against the risk of hacking. Hacking evolves, and is continually seeking new areas for exploitation. Consequently, a more agile response to the threat of hacking is required.

10. **Discuss the origin and meaning of ethical hacking, with reference to ethical hacker profiles and methodology.**

A detailed literature review on the ethical hacking response has been conducted in order to highlight the unique nature of this response. Ethical hacking is the discipline of
using the same tools and techniques used by hackers – with the intent, however, of identifying security vulnerabilities and weaknesses in an organisation’s system defences, towards protecting the organisation against hacker attacks. In contrast to hacking activity, ethical hacking is considered legal, since it is conducted with the organisation’s permission.

Ethical hackers are typically regarded as information security specialists and require the same skills and creativity found in hackers. However, ethical hackers are considered trustworthy, and maintain the highest ethical principles. Three different profiles can be distinguished among ethical hackers: white hat hackers, tiger teams and red teaming. White hat hackers are often part of the hacking community; however, they work towards identifying security vulnerabilities for the greater good of the industry. Tiger teams simply refer to a group of ethical hackers. Red teaming refers to a team tasked with compromising an organisation’s defences, similar to black hat hackers, who would spare no cost in achieving their objective.

Ethical hackers follow a generic methodology, which includes several phases that are very similar in nature to the generic hacker methodology. The primary difference, however, is that an ethical hacker would strictly follow each methodology phase, whereas a hacker would engage in any or all of the methodology phases.

There are various terms used synonymously with the term ethical hacking. This includes vulnerability assessment, which focuses on all the phases of the ethical hacking methodology, except the exploitation and maintenance phases, which are considered the most controversial stages of the ethical hacking methodology. Another term used synonymously with ethical hacking is penetration testing. This approach specifically engages in all the stages of the ethical methodology, including the actual exploitation of vulnerabilities in the organisation’s systems and networks. Ethical hacking assignments can therefore be conducted in levels of intensity, with vulnerability assessment being the more conservative approach, limited to identifying vulnerabilities only, and penetration testing the more aggressive approach, allowing the exploitation of vulnerabilities.

11. **Explore the sometimes controversial practice of ethical hacking, by considering the placement of ethical hackers in an organisation and their supporting skills requirements and qualifications.**
Ethical hackers can be placed either internally or externally to an organisation. There are many factors to consider when making this decision, ranging from the size of the organisation and the complexity of the systems to the sensitivity of the organisation’s information assets. Specialised recruitment practices may also be followed when ethical hackers are hired, to ensure that the organisation does not employ a hacker with a criminal past. Alternatively, an organisation could make use of ethical hacking service providers. Ethical hackers require a similar skillset compared to hackers. Generally, a deep technical understanding of technology is required. Ethical hackers often complete professional ethical hacking qualifications or belong to professional information security bodies.

12. **Explore the advantages, disadvantages and motivation for the need for ethical hacking.**

The literature review has also highlighted several advantages and disadvantages associated with ethical hacking. One of primary advantages of ethical hacking is that it is one of the most effective mechanisms to identify security vulnerabilities and protect an organisation against hacker attacks. It also assists an organisation in determining the likelihood of hacker attacks and averts potential reputational consequences. The hands-on approach of ethical hacking highlights vulnerabilities which can be remediated immediately. One of the disadvantages of ethical hacking is that the simulated hacking activity could negatively affect the organisation’s systems. Confidential information may be disclosed. System and network performance may be affected. Ethical hackers also need to constantly keep up to date with the latest developments in vulnerabilities and information security practices. Ethical hacking tools, often similar to hacking tools, could cause system failure or launch DoS attacks. It is therefore imperative that the ethical hackers comprehend the functioning of the tools and the consequences of their actions.

13. **Explore ethical hacking as a multi-faceted response to hacking. This thesis highlights how ethical hacking can be a response to all the business risks, IT risks and control objectives identified in the thesis.**

It has been established in the literature that ethical hacking can be applied from four perspectives. Firstly, ethical hacking can be used to improve an organisation’s network security posture. It can be used as a complete approach towards improving information security and involves identifying every possible security vulnerability. It can
also be used as part of a larger information security strategy, towards improving the organisation’s system defences. Secondly, ethical hacking can be used to improve application security and decrease software vulnerabilities during software development. This is an effective means of improving software security before deployment of the applications into production. Thirdly, ethical hacking can be used as part of an organisation’s risk management process, in particular when identifying IT risk. This approach provides tangible input into the risk management approach and could assist with the prioritisation of IT risks. Lastly, ethical hacking can be used as a tool to augment other governance responses, such as corporate governance, security technologies and the baseline security configuration. Ethical hacking provides additional insight into the organisation’s security practices and informs senior management of the effectiveness of internal control.

Ethical hacking can be used as a response to all the IT risk themes identified in this thesis. In as much as hacking can increase each IT risk, ethical hacking can be used to test the likelihood of each IT risk occurring and recommend remedial actions. By implication, ethical hacking can be used as a response to the business risks as well, from the perspective of preventing the IT risk of increasing or affecting the business risk. Ethical hacking can also be used to test the achievement of the control objectives identified in this thesis. In comparison with the other responses to hacking identified in this thesis, ethical hacking provides the most comprehensive coverage of IT risk themes. From the literature study, it stands out as a comprehensive response to IT risk and hacking.

14. **Provide a brief overview of banking in South Africa and review the annual results of each of the 16 registered banks in South Africa, towards an understanding of selected governance practices and responses to IT risk and hacking.**

The literature study has highlighted that banks are critically dependent on IT to enable their processes and products. This dependency also introduces risk and fraud. The South African banking sector is a very competitive industry and consists of 16 locally registered banks, while four banks dominate the local market.

Although banks in general subscribe to principles of good corporate governance, the extent to which they disclose this in their annual reports differs among the various competitors. All the banks follow risk management practices, with credit risk, market
risk, operational risk and compliance risk being recognised as the most significant
business risks. There was very limited disclosure of the business risks of human
resource risk, technology risk and physical risk. Very few banks have established an IT
steering committee at board of director level. Not all banks have highlighted IT risk as
a significant business risk. There is very limited disclosure of IT risk themes, except for
business and IT disruption. Hacking and cybercrime were not disclosed by any of the
banks.

More than half of the banks disclosed their IT governance practices, although the
amount of detail provided differs substantially from bank to bank. There is also
inconsistency in terms of what is being reported from an IT governance perspective. In
very few cases has it been disclosed that IT is included in the bank’s risk management
processes. Information security management practices are also not disclosed in most
instances. Software development practices and governance frameworks were
disclosed by only one bank. The use of ethical hacking has also not been highlighted
in any of the annual reports.

10.2.2 Conclusions from the analysis of the questionnaires

A detailed discussion of the outcome of the analysis of the questionnaires was provided in
Chapter 9. This section aims simply to provide a high-level conclusion to the primary
research findings, against each of the primary research objectives identified in section 1.4.

1. Given that hackers often target banks, determine what the responses to hacking
are in the South African banking sector.

The company secretaries regarded the board of directors’ overall response to
cybercrime and hacking as good, despite an apparent lack of skill in dealing with IT
matters. The company secretaries and the individuals responsible for IT indicated that
IT governance practices are used only to some extent to fight cybercrime. The
individuals responsible for IT indicated that their organisation’s response to insider
attacks is not as effective as it should be.

The primary responses to the risk of hacking in the South African banking sector from
the perspective of the company secretaries and individuals responsible for IT include
security technologies, information security management and IT governance. None of
these fully address the risk of hacking.
Employee vigilance was not rated high by the individuals responsible for IT as an effective response to hacker attacks, and this indicates that social engineering attacks have a good likelihood of succeeding at some banks. Software development practices were rated low by the individual responsible for IT, despite the fact that secure software development practices could assist in preventing the exploitation of vulnerable software by hackers.

Ethical hacking has been identified in this thesis as the most comprehensive response to hacking. Ethical hacking is used by most banks as a response, although it was ranked low by the company secretaries and individuals responsible for IT. The company secretaries and the individuals responsible for IT did not recognise the comprehensive nature of ethical hacking as a response. Governance frameworks such as CobiT were also ranked low by the company secretaries, despite being listed in King III. This indicates that governance frameworks are not extensively used as a response to hacking.

In terms of the effectiveness of the responses to hacking, the company secretaries and the individuals responsible for IT highlighted security technologies, information security management, and internal control as the most effective responses to hacking. This study has argued that these are not the most comprehensive responses to IT risk and hacking. The company secretaries and the individuals responsible for IT might therefore have a false sense of security. Software development was rated low by both the company secretaries and the individuals responsible for IT in terms of the effectiveness of the response, which indicates that secure software development practices might be applied by only a few banks.

Only some individuals responsible for IT saw ethical hacking as advantageous in identifying and remediating information security and software vulnerabilities. Ethical hacking has not been commonly accepted as an effective response to hacking in the banking sector yet, and consequently the banking sector may be at risk of being attacked by hackers if it is not using the most effective response to hacking.

The skills levels of ethical hackers are considered a determining factor in the success of ethical hacking assignments by the individuals responsible for IT, which indicates that ethical hacking is either applied incorrectly or that the required skills levels of ethical hackers used by the banking sector are not on par with the expectations of the individuals responsible for IT. Governance frameworks were also rated low in terms of
effectiveness, which indicates that they are not applied effectively as a response to IT risk and hacking.

2. **Determine what the depth of the governance responses to hacking is in the banking sector.**

The company secretaries and individuals responsible for IT were satisfied with the support they received from the board of directors. The company secretaries and individuals responsible for IT were generally satisfied that the board of directors’ overall response to IT risk and cybercrime was good, although this was not the case at three banks. The individuals responsible for IT have highlighted that not all of the boards of directors have fully accepted their IT governance responsibilities, indicating that the response to hacking may not be dealt with by the board of directors. The overall responsibility for IT has only been assigned to a particular board member at five banks. Both the company secretary and the individual responsible for IT have highlighted the board of directors’ lack of IT skills to deal with IT matters, which leads to the delegation of IT matters to other committees. Hacking is on the board of directors’ agenda at only a few banks, and meeting minutes containing IT matters may not reach the board of directors.

The questionnaire respondents have highlighted that security technologies, information security management, internal control and risk management were the most effective responses to hacking. The literature study has however shown that these responses are not the most effective responses to the threat of hacking. Corporate governance, ethical hacking, software development practices and governance frameworks have been highlighted as the least effective response to hacking by the company secretaries and individuals responsible for IT. In contrast, the literature study has highlighted that ethical hacking is the most comprehensive response to hacking. Respondents were therefore unclear as to how those responses can be effectively applied as a response to hacking.

Ethical hacking is used as a response by most banks, although not as extensively as other governance responses. The effectiveness of the ethical hacking response is not fully recognised in the banking sector.
3. Establish whether the board of directors provide sufficient oversight and focus on IT risk in the local banking sector.

The individuals responsible for IT were not as satisfied as the company secretaries with the board of directors’ IT risk oversight role. A possible root cause for this is the lack of IT skills at board of director level. IT risk is mostly delegated to other committees, such as risk management or IT steering committees. IT risk is perhaps not yet treated on equal terms with other business risks. In terms of the different IT risk themes, not all were considered significant by the company secretaries or the individuals responsible for IT, although all can be affected by hacking.

4. Determine whether hacking is considered a threat in the local banking sector.

Hacking is considered a significant risk by the individuals responsible for IT at seven banks. The individuals responsible for IT were less satisfied with the board of directors’ overall response to cybercrime and hacking than the company secretaries were. This indicates that the individuals responsible for IT believe the board of directors should pay closer attention to cybercrime and hacking. This is further supported by the fact that hacking appears on the board of directors’ agenda at only a few banks. The company secretaries were of the opinion that IT governance practices are only used to some extent towards fighting cybercrime. Considering the reliance placed on security technologies as a response to hacking, this indicates that the response to hacking could be more of a tactical response than a more general governance response.

The company secretaries and individuals responsible for IT understood the link between IT risk and the business risks, technology risk, business continuity risk, operational risk and disaster recovery. However, the link between IT risk and the other business risks, such as physical risk, human resource risk, market risk, credit risk, reputational risk and compliance risk is not clearly understood, which implies that these could be affected by hacking. The company secretaries and the individuals responsible for IT agreed that hacking strongly increases the IT risk themes of logical access risk, IT systems risk, IT continuity risk and cybercrime (including hacking). However, considering the low ranking of other IT risks, such as physical access risk, IT human resource risk, communications failure and lack of software development, the company secretaries and the individuals responsible for IT do not fully comprehend yet how hacking can be a threat to other IT risk themes.
A few individuals responsible for IT did not believe hacking is a significant threat to their organisation. This implies that the risk of hacking is underestimated at some banks. The individuals responsible for IT were aware of the increase of criminal awareness among hackers, as a key driver towards the increase of hacking in the banking sector. The use of security technologies, such as firewalls, implies a tactical response and daily on-going protection against hacker attacks. The risk of the insider threat is definitely underestimated, which is highlighted by less focus being placed on physical risk and human resource risk than on other business risks. The motivations of hackers were not understood by the individuals responsible for IT, which indicates that the risk of hacktivism is underestimated.

5. **Determine the extent to which banks make use of ethical hacking as a possible response to the threat of hacking.**

Ethical hacking has been identified in this thesis as the most comprehensive response to hacking. Most banks have indicated that they have made use of ethical hacking at some point. Given the responses elicited as to the use and effectiveness of the various responses to hacking, it is clear ethical hacking is not used as a primary response to the threat of hacking in the banking sector. Ethical hacking has been regarded as an effective response to hacking in general, although this contradicts the ranking of ethical hacking in relation to other responses to hacking. It is understood that ethical hacking can be used to identify security vulnerabilities and to test internal control against hacker attacks; however, it would appear, perhaps, that ethical hacking is used instead on an ad-hoc basis in the banking sector.

The skills level of the ethical hacker was seen as a determining factor in the success of an ethical hacking assignment, although generally the individuals responsible for IT were not concerned that ethical hacking would adversely affect the bank’s systems. The primary advantage associated with ethical hacking was the identification and remediation of information security and software vulnerabilities.

### 10.3 RECOMMENDATIONS

Given the outcome of the literature study and the empirical fieldwork, the following recommendations are made in terms of the various topics discussed in this thesis.
10.3.1 Recommendations associated with the meaning of the concept hacking

Awareness and education is required in the banking sector to enhance the general understanding of the concepts of hacking, hacker profiles, hacker skills levels and ethical viewpoints. In particular, the motives and objectives of hackers and the extent to which these could increase the hacker threat need to be highlighted.

The exact extent of the hacker threat to the banking sector needs to be determined. Perhaps the disclosure of hacking incidents should be legislated, seeing that the banking sector will be reluctant to share this information. A differentiation should be made between insider attacks and external hacker attacks in the disclosure. A cybercrime forum or workgroup in the banking sector could assist in sharing best practice and lessons learned. Collaboration between banks could lead to the identification of hackers and cybercriminals. This could also lead to the prevention of hacker attacks against other banks.

Greater awareness needs to be created in the banking sector regarding the reality of hacking being both a risk and an event. The hacking threat needs to be managed via both preventative and detective controls.

10.3.2 Recommendations associated with the link between IT risk, business risk and hacking

Awareness and education is required in the banking sector regarding the link between IT risk and hacking. In particular a detailed understanding of the various IT risk themes and how they can be affected by various types of hacking attacks need to be emphasised. Similarly, the links between business risks, IT risk themes and hacking also need to be highlighted.

10.3.3 Recommendations associated with the general responses to hacking

Greater awareness is required in the banking sector as to how corporate governance can be applied as a response to hacking, in particular at the board of director level. An organisation’s corporate governance duties are not fulfilled with a singular response to hacking. At a minimum, corporate governance calls for risk management, internal control and IT governance. Furthermore, the role that ethical hacking plays in the context of these responses needs to be emphasised. Further guidance on these matters is required in the banking sector.
More consideration should be given to specialised risk management frameworks, such as NIST Special Publication 800-30. Frameworks such as these combine multiple responses – in this case risk management and ethical hacking. This will ease the adoption of responses, such as ethical hacking.

IT governance is a complex subject, with various options for implementation. Simplification of the concept is required to make it more palatable to smaller organisations. IT governance frameworks, such as CobiT, do not explicitly include the use of ethical hacking. The use of ethical hacking as part of IT governance is therefore encouraged. The involvement of the board of directors in establishing and participating in IT governance practices also needs to be encouraged.

The link between information security management as a response and ethical hacking as a response to the risk of hacking is understated. Information security management material tends to refer to ethical hacking as a standalone technique, with limited application as a component of information security management, rather than truly integrating ethical hacking into the various subject areas found in information security management.

Greater awareness needs to be created in the banking sector as to the limited application of technical security solutions in mitigating the risk of hacking. There is a false sense of security that exists in the banking sector as to the effectiveness of technical security solutions such as firewalls.

10.3.4 Recommendations associated with the concept of ethical hacking

The banking sector should standardise the use of ethical hacking terminology. This will provide greater clarity in terms of the scope and intent of ethical hacking assignments.

The use of ethical hacking should be encouraged for organisations relying significantly on IT to enable their daily operations. Moreover, the use of ethical hacking should be mandatory for organisations holding confidential client details or safeguarding client funds. Again, legislation might be the only mechanism of enforcing the use of ethical hacking.

Ethical hacking is a skill than could be mastered by existing staff. Trustworthy employees with a strong technical skillset could be good candidates. Not all ethical hacking techniques are necessarily complex in nature and could be used by IT departments to improve their control environment.
Organisations need to be wary when appointing white hat hackers. There is a clear distinction between ethical hackers and white hat hackers. Recruitment guidelines should be compiled to assist the banking sector in distinguishing between ethical hackers and white hat hackers. Particular emphasis should be placed on the necessity of ethical hacking qualifications and membership of professional bodies.

Ethical hacking can be applied as part of various disciplines. Greater awareness of the various uses of ethical hacking in the banking sector is required. In particular, ethical hacking should be used extensively as part of several phases of a typical SDLC, in particular during the testing phase and shortly before deployment into production. The use frameworks, such as OWASP and SAMM, should be encouraged. Ethical hackers can provide training to software developers and system administrators in terms of sensitive attack vectors and coding best practices.

Clear guidelines as to the management of ethical hacking assignments, in particular to avoid the associated disadvantages, should be compiled for use within the banking sector.

Ethical hackers potentially have a unique understanding of the organisation’s network and system defences. They might be able to make recommendations regarding the general improvement and design of network and system infrastructure, in particular from a secure system design perspective. This insight should not be underestimated, and participation by ethical hackers in design forums and architectural review committees should be encouraged.

Ethical hacking should not be limited to, for example, technical exploitation of software vulnerabilities. Hackers are very creative in finding ways to break into an organisation, which include both technical and non-technical techniques. The realisation that ethical hacking should also include non-technical techniques is not fully accepted yet. Ethical hacking is a broader discipline that includes the testing of general security practices and provides broader input into aspects such as:

- Security architecture and design.
- Effectiveness of information security processes.
- Effectiveness of physical access controls (physical risk).
- Assessment of staff vigilance and intruder detection (human resources risk).
- Effectiveness of incident management and business continuity procedures to deal with significant hacking incidents.
The use of ethical hacking in combination with other risk management and assurance activities is encouraged, as this will provide greater assurance over the organisation’s defence against hacker attacks. Ethical hacking used during forensic investigations could assist with the collection of evidence. Ethical hacking can also be used by internal audit departments to test the information security of platforms and provide convincing evidence, rather than theoretical assumptions, regarding the possible impact of control weaknesses.

10.3.5 Recommendations associated with the disclosure practices in the local banking sector

Clarity is required regarding the definition of operational risk and whether the banking sector interprets the “systems” component of operational risk as IT or not. Similarly, clarification is required regarding the interpretation of technology risk and whether it includes IT risk as a sub-component. Given that this thesis has highlighted the significance of IT and IT risk within the business world of today, it is argued that IT risk should be recognised as a separate risk in order to ensure that it receives enough attention from the board of directors.

The disclosure of IT governance practices is not consistent in the banking sector. Clear guidance could be provided for IT governance topics that should be disclosed in the annual results of banks. Very few banks have disclosed information security or cybercrime issues. Greater transparency regarding these matters is required from the banking sector.

10.3.6 Recommendations associated with the responses by the company secretaries and individuals responsible for IT

Greater ownership of IT matters at the board of directors level should be encouraged. IT governance responsibilities at some banks at the board of directors level do not always carry sufficient priority. IT risks are not always assigned the same weight as other business risks. Guidance should be provided for IT matters and IT governance topics that should be covered, specifically by the board of directors in the banking sector. IT governance best-practice guidelines for smaller banking operations in particular should be compiled. Company secretaries should ensure that the board of directors is adequately trained in IT matters and should schedule training for the board of directors in the latest risks and advances in IT, at least annually.

With the reliance of business on IT, it is not enough for the board of directors to focus only on high-level IT matters. Sufficient coverage of IT needs to be incorporated into the agenda
of the board, even when an IT steering committee has been established. It is recommended that the CIO attends the board of directors’ sessions where IT matters are discussed. The responsibility for IT should be assigned to a particular member of the board who is suitably qualified for the role. It is also recommended that IT steering committees are established at the board of directors level to ensure more focused attention on IT issues. The board of directors should always receive the meeting minutes or briefing notes of IT steering committees, or other committees dealing with IT matters.

Greater clarity is required in the banking sector as to how business risks, such as human resource risk, market risk, credit risk and physical risk, can be increased by IT risks such as hacking. This awareness should in particular be increased at the board of directors level. Also, greater awareness regarding the ways hacking could increase IT risk themes, such as IT human resources risk, physical access risk and lack of software development, is required in the banking sector. Hacking should at least be covered as an IT risk on the agenda of the board of directors.

The use of standards and frameworks such as CobiT is encouraged, as this will lead to greater maturity in IT governance, information security and risk management practices in the banking sector. The use of corporate governance as a response to hacking should be clarified. Ethical hacking should be used more extensively as a response to hacking in the banking sector. Currently it may find only limited application, which implies that the full benefits of ethical hacking are not achieved.

The skills level of an ethical hacker is a determining factor in the success of an ethical hacking assignment. Various ethical hacking qualifications are available; however, more formal grading and certification of levels of ethical hacker skills can be incorporated in tertiary education.

Persuading management of the threat of hacking has not been identified as a primary advantage. However, showing the implications of system breaches, by for example “stealing” data during an ethical hacking assignment, could make management and even the board of directors aware of the actual consequences and business impact of hacker breaches. Tangible results of what could have happened during an actual hacker breach are more convincing than just making reference to the technical vulnerability exploited.

Recruitment guidelines for ethical hackers can be compiled for the banking sector to ensure that only trustworthy ethical hackers are deployed. The recruitment process should include
background checks and identify involvement in possible white hat activity, which may highlight unsuitability for an ethical hacker position.

10.4 AREAS FOR FURTHER RESEARCH

Research can be conducted on the reasons why the board of directors does not pay the same attention to IT risk as it does to other business risk. Comparisons can be drawn between boards of directors who do focus on IT risk and those who do not, and the effect this may have on the profitability of the organisation.

Research can also be conducted on the adoption and embedding of IT governance in the banking sector. The level of maturity of IT governance can be determined. The role of the board of directors in enabling IT governance can also be explored, particularly seeing that the board of directors does not always accept this responsibility.

Although this study focused primarily on crimes committed by hackers, the research can be extended to cybercrime in general. The wider impact of cybercrime on business risk and IT risk can be explored, and appropriate responses can be identified.

The exact fit of ethical hacking within the context of IT governance can be considered. More in-depth research into an ethical hacking methodology and alignment with other best-practice frameworks can be considered. In particular, how ethical hacking can support many of the disciplines found in an IT department, such as security architecture, system development of secure software, testing of network defences, could be studied in more detail. A generic framework for ethical hacking can be defined, followed by more detailed guidance on the areas in which ethical hacking can be used. Mappings can be compiled between popular frameworks, such as CobiT and ISO 27002, to determine where ethical hacking can used to complement those frameworks. The effectiveness of ethical hacking versus that of other responses to hacking can be studied in greater detail in order to provide an understanding of the exact coverage that can be achieved with various responses.

Research can also be done into the real impact of ethical hacking on a business, such as actual system impact or system downtime. This in turn could be compared to potential losses averted due to increasing system security. The research in this study can also be extended to the public sector, focussing specifically on the governance processes in place to direct the appropriate response in the public sector.
The overlap between ethical hacking and IT auditing can be explored. Ethical hacking can include IT auditing, and IT auditors can make use of ethical hacking in their assurance work.

10.5 CONCLUSION

This thesis explored governance responses to hacking in the South African banking sector. The results of the literature study and the questionnaires in the banking sector have been summarised against the objectives set out in Chapters 1 and 8 of this study. The strong link between business risk, IT risk and hacking has been established. Various responses to the risk of hacking have been identified, but it has been demonstrated that none is as effective as ethical hacking. Hacking is considered a significant threat to the banking sector; however, the most effective response, ethical hacking, is not yet being used extensively as a response. Boards of directors need to pay more attention to IT risks, including the risk of hacking. They need to be significant role-players in the response to the hacking threat.

Further research into the implications of ethical hacking, towards proliferation of this response in the banking sector, is required.


AICPA. See American Institute of Certified Public Accountants, Inc.

AIRMIC. See The Association of Insurance and Risk Managers.


*Reference List*


Association of Insurance and Risk Managers, The. (AIRMIC), ALARM the National Forum for


BERR. See Department for Business, Enterprise & Regulatory Reform.


CICA. See The Canadian Institute of Chartered Accountants.

CIS. See Center for Internet Security.


COSO. See Committee of Sponsoring Organizations of the Treadway Commission.


CREST. See Council of Registered Ethical Security Testers.


CSSA. See Chartered Secretaries South Africa.


Johannesburg: University of Johannesburg.


Ernst & Young. (2010). *IT risk and assurance*. Available


EYGM Limited. See Ernst & Young Global Limited.


FFIEC. See Federal Financial Institutions Examination Council.


Google. (2012). “internet banking” number of users “South Africa”. Available from: http://www.google.co.za/#sclient=psy-ab&q=%22internet+banking%22+number+of+users+%22South+Africa%22&oq=%22internet+banking%22+number+of+users+%22South+Africa%22&aq=f&aql=&gs_l=serp.3...0.0.0.152641.0.0.0.0.0.0.0.0.0.0.0.1q4Nk-oo9E&pbx=1&bav=on.2,or.r_gc.r_pw.,cf.osb&fp=dc468175e869d5f6&biw=1024&bih=601 (Accessed 1 May 2012).


Han, S. J. (2003). *Demystifying security tools. should I use commercial or freeware?* Information Security Reading Room. SANS Institute.


IBM Corporation. See International Business Machines Corporation.

iC³. See Internet Crime Complaint Centre.

ICSA. See Institute of Chartered Secretaries and Administrators.
IFAC. See International Federation of Accountants.

IIA, The. See The Institute of Internal Auditors.

IIARF. See The Institute of Internal Auditors Research Foundation.


---

**Reference List**


IoD. See Institute of Directors of Southern Africa.

IRBA. See Independent Regulatory Board for Auditors.

IRMSA. See Institute of Risk Management South Africa.


ISACF. See Information Systems Audit and Control Foundation.


ISO. See International Organization for Standardization.


ITGI. See IT Governance Institute.


IT Governance Institute. (ITGI). (2008e). *Unlocking value. an executive primer on the critical
role of IT governance. Illinois, USA: IT Governance Institute.


itSMF. See IT Service Management Forum.


JSE. See Johannesburg Stock Exchange.


Luper, B. (2002). Be prepared: if you don’t already have a risk management plan addressing all facets of your organization, it’s time to get one. *Association Management*, 54(7):59-64.


*Reference List*


073/t/2 (Accessed 3 October 2010).


MIS Corporate Defence Solutions Ltd. (2000). *An overview of network security analysis and penetration testing. A guide to computer hacking and preventative measures*. Available from:


NIST. See National Institute of Standards and Technology.


OECD. See Organisation for Economic Co-operation and Development.


OSVDB. See Open Source Vulnerability Database.


PCI. See Payment Card Industry.


PMI. See Project Management Institute, Inc.


PTES. *See The Penetration Testing Execution Standard.*


PwC. *See PricewaterhouseCoopers.*


Association for Accounting Education & Research (IAAER), 26-29 June 2011: Fancourt, George, South Africa.


SACFIS. See South African Centre for Information Security.

SAICA. See South African Institute of Chartered Accountants.


SARB. See South African Reserve Bank.


*Reference List*


Van Tonder, C. L. (2006). Towards a minimum conceptualisation of ethical organisational


Dear <<Participant>>

PARTICIPATE IN RESEARCH ON IT GOVERNANCE AND IT RISK

The South African banking sector is well developed, effectively regulated and regarded as a world leader in many respects. But the sector is also dynamic, and boards of directors are constantly faced with challenges – none more so than those posed by Basel III, King III and advances in technology. Given the banking sector’s dependency on information technology (IT) and the IT risks that it faces, you as company secretary have valuable insights into the governance practices followed by your board of directors and by senior executives tasked with IT governance.

Your views are also critical to the successful outcome of a doctoral study in auditing prepared by Mr Christiaan Roos at the University of Johannesburg. Christiaan has more than 10 years’ experience as an IT auditor within the banking sector and has presented on the topic of ethical hacking, IT governance and continuous auditing at several conferences and seminars.

Therefore, we request 15 minutes of your time to complete the short questionnaire attached hereto. Your response as custodian of governance practices in your organisation, as emphasised by King III and legislated by the Companies Act, is extremely valuable to this doctoral study on governance responses to IT risk and hacking at South African registered banks. More so as you will be one of only 16 company secretaries of registered banks in South Africa targeted in this research. Should you require more information about the research or the questionnaire, you are welcome to contact Christiaan: 083 333 1234 or roos@emailadress.co.za.

Should you not be able to complete the questionnaire, we would appreciate your response to that effect for control purposes.

Lastly, we would appreciate your assistance in providing the name and contact details of the person in your organisation entrusted with IT governance to Christiaan telephonically, via email or through the questionnaire, as his research will also document the views of these individuals on IT governance and the risk of hacking.
Yours sincerely,

Professor Thea Voogt
D Com, CA(SA)
Supervisor

Tel: +27 11 559 1234
Email: voogt@uj.ac.za

Professor Ben Marx
D Com, CA(SA)
Co-supervisor

Physical address:
First floor, Madibeng building
Auckland Park Kingsway Campus
QUESTIONNAIRE TO THE COMPANY SECRETARY

INSTRUCTIONS:

1. You are kindly requested to complete the entire questionnaire.
2. The questionnaire can be completed online, manually or electronically.
   b. Manually:
      - Detailed instructions on how to complete the questionnaire are provided within the phrasing of each question. Most of the answers are simply given by ticking a box.
      - Once completed, please return the questionnaire in the self-addressed envelope to 373A Piet Hugo Street, Eldoraigne X17, 0157, South Africa or fax it to 086 584 9414.
   c. Electronically (the MS Word document):
      - Detailed instructions on how to complete the questionnaire are provided within the phrasing of each question. Most of the answers are simply given by scrolling down the questionnaire and clicking the relevant box with your mouse.
      - Please ensure that you select **only one answer per row**, where appropriate.
      - To change your answer in any of the boxes, simply click on the box ticked incorrectly to clear it, and re-select your answer by clicking on the correct box.
      - Please save the completed questionnaire to disk, before returning it via email to the researcher at rooscj@webafrika.org.za.
      - You can also print the completed questionnaire and fax or post it to the address or fax number provided above.
3. You are kindly requested to complete the questionnaire by 15 January 2012.
4. You are encouraged to provide additional comments in the space provided.
5. Should you wish to contact Christiaan Roos, you can do so at 083 3061543.

Individual responses will not be identified.
Responses will be used to produce aggregate results.

Your co-operation is appreciated.
Thank you in anticipation.
1. Your corporate governance role

1.1 Answer yes or no to the following questions:

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you get enough support from the board of directors to perform your corporate governance responsibilities?</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Do you have the freedom to add new corporate governance issues to the agenda of the board?</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Do you believe that enough guidance is provided by professional and regulatory bodies in terms of your corporate governance responsibilities?</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

1.2 Any additional comments:

…………………………………………………………………………………………………………………………………………
…………………………………………………………………………………………………………………………………………
…………………………………………………………………………………………………………………………………………
…………………………………………………………………………………………………………………………………………

2. Your views on the board and IT governance

2.1 Indicate the extent to which you agree with the following statements in your organisation. Select or click one option in each row below:

<table>
<thead>
<tr>
<th>Statement</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>The board of directors takes responsibility for IT governance.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The board of directors effectively address IT governance.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The board members have the necessary skills to deal with IT matters.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT governance is a key component of corporate governance in our organisation.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT governance is high on the board’s agenda.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Our IT governance practices compare favourably with that of our competitors.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The board’s overall response to IT risk is good.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The board’s overall response to cybercrime is good.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The board’s overall response to hacking is good.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2.2 Any additional comments:

…………………………………………………………………………………………………………………………………………
…………………………………………………………………………………………………………………………………………
…………………………………………………………………………………………………………………………………………
…………………………………………………………………………………………………………………………………………
3. Your views on IT in your business

3.1 Indicate the extent to which you agree with the following statements in your organisation. Select or click one option in each row below:

1 = Agree completely
2 = Agree to a large extent
3 = Agree to a moderate extent
4 = Agree to a lesser extent
5 = Don’t agree at all

<table>
<thead>
<tr>
<th>Statement</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our ability to deal with IT challenges is good.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Our ability to deal with IT risk is good.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT plays a key enabling role in our products and services.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Our IT governance practices are key to fighting cybercrime.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3.2 Any additional comments:

................................................................................................................
................................................................................................................
................................................................................................................
................................................................................................................

4. Incorporating IT governance into your organisation

4.1 Rank the following factors which may have contributed towards the incorporation of IT governance practices in your organisation. Write or type the numbers 1 (most important) to 5 (least important) in the column provided. Use the numbers 1 to 5 only once.

<table>
<thead>
<tr>
<th>Rank</th>
<th>Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The culture of the organisation</td>
</tr>
<tr>
<td></td>
<td>Regulatory requirements or legislation</td>
</tr>
<tr>
<td></td>
<td>Achieving business objectives or strategy</td>
</tr>
<tr>
<td></td>
<td>Industry norm and practice</td>
</tr>
<tr>
<td></td>
<td>Growth in complexity of the IT function</td>
</tr>
</tbody>
</table>

4.2 Any additional comments:

................................................................................................................
................................................................................................................
................................................................................................................
................................................................................................................

........................................... UNIVERSITY OF JOHANNESBURG ...........................................
5. The one person responsible for IT

5.1 Answer yes or no to the following questions:

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Has your organisation appointed an individual responsible for the management of IT?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If no, indicate who accepts overall responsibility for the management of IT. Specify in the field provided:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you think the individual responsible for IT is suitably qualified to deal with IT governance?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you think the individual responsible for IT is suitably experienced to deal with IT governance?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the individual responsible for IT invited to attend board of directors meetings?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Has the overall responsibility for IT been assigned to a particular board member?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5.2 Indicate how the individual responsible for IT is referred to. Select or click one option below or provide the title in the block provided (Other):

- Chief Information Officer (CIO)
- Chief Technology Officer (CTO)
- Head of IT
- Other (please provide)

5.3 Whom does the person responsible for IT report to? Select or click one option below:

- Chief Operating Officer (COO)
- Chief Financial Officer (CFO)
- Chief Executive Officer (CEO)
- Board of directors
- Audit committee
- Other (please provide)

5.4 Indicate the extent to which you agree with the following statements. Select or click one option in each row below:

1 = Agree completely
2 = Agree to a large extent
3 = Agree to a moderate extent
4 = Agree to a lesser extent
5 = Don't agree at all

<table>
<thead>
<tr>
<th>Statement</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>The individual responsible for IT understands how to integrate IT governance into the business.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The individual responsible for IT ensures that IT solutions meet the strategic objectives of the organisation.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5.5 Any additional comments:

........................................................................................................................................................................
........................................................................................................................................................................
........................................................................................................................................................................
6. **Contact details**

Just as your views are critical to the outcome of this study, so too are the views of the individual responsible for IT. Please provide the name and contact details of the individual responsible for IT.

-------------------------------------------------------------------------------------------------------------------------------------

Contact details:  
(office number)  
(email)  

*Kindly note that this information will be treated as confidential.*

7. **Board committees and IT**

7.1 Which board committees deal with IT matters? Specify in the field provided.

-------------------------------------------------------------------------------------------------------------------------------------

-------------------------------------------------------------------------------------------------------------------------------------

-------------------------------------------------------------------------------------------------------------------------------------

7.2 Which other non-board committees deal with IT matters? Specify in the field provided.

-------------------------------------------------------------------------------------------------------------------------------------

-------------------------------------------------------------------------------------------------------------------------------------

-------------------------------------------------------------------------------------------------------------------------------------

7.3 Answer yes or no to the following questions:

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are the briefing notes or minutes relating to IT matters discussed at committees, submitted to the board of directors?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is IT governance a standing agenda item for the board of directors?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

7.4 Indicate the frequency of IT matters being included on the boards’ agenda. Select or click one box below.

<table>
<thead>
<tr>
<th>Frequency</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Never</td>
<td></td>
</tr>
<tr>
<td>Case by case</td>
<td></td>
</tr>
<tr>
<td>Routinely</td>
<td></td>
</tr>
<tr>
<td>Do not know</td>
<td></td>
</tr>
</tbody>
</table>

7.5 Any additional comments:

-------------------------------------------------------------------------------------------------------------------------------------

-------------------------------------------------------------------------------------------------------------------------------------

-------------------------------------------------------------------------------------------------------------------------------------
8. Your views on business risk and IT risk

8.1 Indicate the extent to which you think IT risk is linked to each of the risks below in your organisation. Select or click one option in each row below:

<table>
<thead>
<tr>
<th>Risk</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operational risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Human resource risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technology risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business continuity risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disaster recovery risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credit risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Market risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reputational risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

8.2 Any additional comments:

........................................................................................................................................................................

........................................................................................................................................................................

........................................................................................................................................................................

........................................................................................................................................................................

9. Your views on hacking

9.1 Hacking is the act of breaking into an organisation’s systems, without authorisation and with malicious intent. Cybercrime refers to a collection of computer related crime, which includes for example hacking, malware and phishing. Indicate the extent to which you think hacking will increase each of the following IT risks. Select or click one option in each row below:

<table>
<thead>
<tr>
<th>Risk</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical access risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT non-compliance risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT continuity risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lack of software development</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cybercrime</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical access risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT human resources risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT systems risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communications failure</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
9.2 Any additional comments:

……………………………………………………………………………………………………………………………………
……………………………………………………………………………………………………………………………………
……………………………………………………………………………………………………………………………………
……………………………………………………………………………………………………………………………………

10. Your views on general responses to hacking

10.1 Indicate the extent to which the general responses below address the risk of hacking in your organisation. Select or click one option in each row below:

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate governance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal control</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT governance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Governance frameworks, such as CobiT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Applying service and quality management, such as ITIL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information security management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software development practices</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ethical hacking</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security technologies, such as firewalls</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

10.2 Indicate how effective each of the general responses to hacking is in your organisation. Select or click one option in each row below:

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate governance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal control</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT governance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Governance frameworks, such as CobiT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Applying service and quality management, such as ITIL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information security management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software development practices</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ethical hacking</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security technologies, such as firewalls</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
10.3 Any additional comments:

........................................................................................................................................
........................................................................................................................................
........................................................................................................................................
........................................................................................................................................

11. IT disclosure

11.1 Answer yes or no to the following statements:

<table>
<thead>
<tr>
<th>Statement</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>There is clear guidance available on what should be reported in the annual results from an IT governance perspective.</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>IT governance related disclosure in our most recent annual report is adequate.</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>IT governance related disclosure will increase in our future annual reports.</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

11.2 Any additional comments:

........................................................................................................................................
........................................................................................................................................
........................................................................................................................................
........................................................................................................................................

Thank you for participating!
Dear <<Participant>>

PARTICIPATE IN RESEARCH ON IT GOVERNANCE AND IT RISK

The South African banking sector is well developed, effectively regulated and regarded as a world leader in many respects. But the sector is also dynamic, and boards of directors are constantly faced with challenges – none more so than those posed by Basel III, King III and advances in technology. Given the banking sector’s dependency on information technology (IT) and the IT risks that it faces, you as a business leader in the industry responsible for IT are well positioned to provide clear insights into IT governance and how you and your board of directors respond to IT governance and the risk of hacking.

Your views are also critical to the successful outcome of a doctoral study in auditing prepared by Mr Christiaan Roos at the University of Johannesburg. Christiaan has more than 10 years’ experience as an IT auditor within the banking sector and has presented on the topic of ethical hacking, IT governance and continuous auditing at several conferences and seminars.

Therefore, we request 15 minutes of your time to complete the short questionnaire attached hereto. Your response as senior executive responsible for IT in one of only 16 locally registered banks is extremely valuable to this doctoral study on governance responses to IT risk and hacking at South African registered banks.

Should you require more information about the research or the questionnaire, you are welcome to contact Christiaan: 083 333 1234 or roos@emailaddress.co.za.

Should you not be able to complete the questionnaire, we would appreciate your response to that effect for control purposes.

Yours sincerely,
QUESTIONNAIRE TO THE INDIVIDUAL RESPONSIBLE FOR IT

INSTRUCTIONS:

1. You are kindly requested to complete the entire questionnaire.
2. The questionnaire can be completed online, manually or electronically.
   b. Manually:
      - Detailed instructions on how to complete the questionnaire are provided within the phrasing of each question. Most of the answers are simply given by ticking a box.
      - Once completed, please return the questionnaire in the self-addressed envelope to 333 Joe Soap Street, Eldoraigne X17, 0157, South Africa or fax it to 086 555 1234.
   c. Electronically (the MS Word document):
      - Detailed instructions on how to complete the questionnaire are provided within the phrasing of each question. Most of the answers are simply given by scrolling down the questionnaire and clicking the relevant box with your mouse.
      - Please ensure that you select only one answer per row, where appropriate.
      - To change your answer in any of the boxes, simply click on the box ticked incorrectly to clear it, and re-select your answer by clicking on the correct box.
      - Please save the completed questionnaire to disk, before returning it via email to the researcher at roos@emailaddress.co.za.
      - You can also print the completed questionnaire and fax or post it to the address or fax number provided above.
3. You are kindly requested to complete the questionnaire by 31 January 2012.
4. You are encouraged to provide additional comments in the space provided.
5. Should you wish to contact Christiaan Roos, you can do so at 083 333 1234.

Individual responses will not be identified.
Responses will be used to produce aggregate results.

Your co-operation is appreciated.
Thank you in anticipation.

[Logo of University of Johannesburg]
## 1. Your role in the organisation

### 1.1 Indicate the extent to which you agree with the following statements. Select or click one option in each row below:

<table>
<thead>
<tr>
<th>Statement</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>The board of directors support me in my IT governance role.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I have sufficient resources to attend to IT governance.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The board of directors take my views seriously.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I have sufficient opportunity to be heard at board committees.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 1.2 Any additional comments:

…………………………………………………………………………………………………………..

…………………………………………………………………………………………………………..

…………………………………………………………………………………………………………..

…………………………………………………………………………………………………………..

## 2. Your views on the board and IT governance

### 2.1 Indicate the extent to which you agree with the following statements in your organisation. Select or click one option in each row below:

<table>
<thead>
<tr>
<th>Statement</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>The board of directors takes responsibility for IT governance.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The board of directors effectively address IT governance.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The board members have the necessary skills to deal with IT matters.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT governance is a key component of corporate governance in our organisation.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT governance is high on the board’s agenda.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Our IT governance practices compare favourably with that of our competitors.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The board’s overall response to IT risk is good.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The board’s overall response to cybercrime is good.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The board’s overall response to hacking is good.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2.2 Any additional comments:

______________________________________________________________________________________________________________________________________________________________________________________

______________________________________________________________________________________________________________________________________________________________________________________

______________________________________________________________________________________________________________________________________________________________________________________

3. Your views on IT in your business

3.1 Indicate the extent to which you agree with the following statements in your organisation. Select or click one option in each row below:

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  = Agree completely</td>
<td>2  = Agree to a large extent</td>
<td>3  = Agree to a moderate extent</td>
<td>4  = Agree to a lesser extent</td>
<td>5  = Don’t agree at all</td>
</tr>
</tbody>
</table>

- Our ability to deal with IT challenges is good. [ ] [ ] [ ] [ ] [ ]
- Our ability to deal with IT risk is good. [ ] [ ] [ ] [ ] [ ]
- IT plays a key enabling role in our products and services. [ ] [ ] [ ] [ ] [ ]
- Our IT governance practices are key to fighting cybercrime. [ ] [ ] [ ] [ ] [ ]

3.2 Any additional comments:

______________________________________________________________________________________________________________________________________________________________________________________

______________________________________________________________________________________________________________________________________________________________________________________

______________________________________________________________________________________________________________________________________________________________________________________

4. Incorporating IT governance into your organisation

4.1 Rank the following factors which may have contributed towards the implementation of IT governance practices in your organisation. Write or type the numbers 1 (most important) to 5 (least important) in the column provided. Use the numbers 1 to 5 only once.

<table>
<thead>
<tr>
<th>Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>The culture of the organisation.</td>
</tr>
<tr>
<td>Regulatory requirements or legislation.</td>
</tr>
<tr>
<td>Achieving business objectives or strategy.</td>
</tr>
<tr>
<td>Industry norm and practice.</td>
</tr>
<tr>
<td>Growth in complexity of the IT function.</td>
</tr>
</tbody>
</table>
4.2 Any additional comments:

……………………………………………………………………………………………………………………………………………………………………

……………………………………………………………………………………………………………………………………………………………………

……………………………………………………………………………………………………………………………………………………………………

……………………………………………………………………………………………………………………………………………………………………

5. Your views on business risk and IT risk

5.1 Indicate the extent to which you think IT risk is linked to each of the risks below in your organisation. Select or click one option in each row below.

<table>
<thead>
<tr>
<th>1 = To a large extent</th>
<th>2 = To a moderate extent</th>
<th>3 = To a small extent</th>
<th>4 = Not at all</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical risk</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operational risk</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Human resource risk</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technology risk</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business continuity risk</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disaster recovery risk</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credit risk</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Market risk</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance risk</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reputational risk</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5.2 Any additional comments:

……………………………………………………………………………………………………………………………………………………………………

……………………………………………………………………………………………………………………………………………………………………

……………………………………………………………………………………………………………………………………………………………………

……………………………………………………………………………………………………………………………………………………………………

6. Your views on hacking

6.1 Hacking is the act of breaking into an organisation’s systems, without authorisation and with malicious intent. Cybercrime refers to a collection of computer related crime, which includes for example hacking, malware and phishing. Indicate the extent to which you agree with the following statements in your organisation. Select or click one option in each row below:
Annexure D

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

1 = Agree completely  
2 = Agree to a large extent  
3 = Agree to a moderate extent  
4 = Agree to a lesser extent  
5 = Don’t agree at all

| Hacking is a significant risk in our organisation. | ☐ | ☐ | ☐ | ☐ | ☐ |
| As an organisation, we are responsible for client side security against hacking. | ☐ | ☐ | ☐ | ☐ | ☐ |
| As an organisation, we should take responsibility for phishing attacks against clients. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Hacking is on the board’s agenda. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Hacking significantly increases our organisation’s reputational risk. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Hacking is a perceived risk as opposed to a real risk. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Our protection against hacker attacks from inside the organisation is good. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Hacking should be prevented. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Hacking should be detected. | ☐ | ☐ | ☐ | ☐ | ☐ |
| The skills level of a hacker affects the response to his attacks. | ☐ | ☐ | ☐ | ☐ | ☐ |
| The moral viewpoint of a hacker affects the response to his attacks. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Our risk of hacker attack from inside the organisation is greater than the external risk. | ☐ | ☐ | ☐ | ☐ | ☐ |

6.2 Indicate the extent to which you think hacking will increase each of the following IT risks. Select or click one option in each row below:

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

1 = To a large extent  
2 = To a moderate extent  
3 = To a small extent  
4 = Not at all

| Physical access risk | ☐ | ☐ | ☐ | ☐ |
| IT non-compliance risk | ☐ | ☐ | ☐ | ☐ |
| IT continuity risk | ☐ | ☐ | ☐ | ☐ |
| Lack of software development | ☐ | ☐ | ☐ | ☐ |
| Cybercrime | ☐ | ☐ | ☐ | ☐ |
| Logical access risk | ☐ | ☐ | ☐ | ☐ |
| IT human resources risk | ☐ | ☐ | ☐ | ☐ |
| IT systems risk | ☐ | ☐ | ☐ | ☐ |
| Communications failure | ☐ | ☐ | ☐ | ☐ |

6.3 Rate the effectiveness of your organisation’s responses to hacker attacks by ticking one appropriate response in each row:

<table>
<thead>
<tr>
<th>Very Good</th>
<th>Good</th>
<th>Fair</th>
<th>Poor</th>
<th>Very Poor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical response</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Technical response</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Employee vigilance</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Overall response</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>
6.4 Rank the following factors which may lead to hacking becoming a greater risk in the banking sector in the future. Write or type the numbers 1 (most important) to 5 (least important) in the column provided. Use the numbers 1 to 5 only once.

<table>
<thead>
<tr>
<th>Rank</th>
<th>General accessibility to hacking tools.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Dependency of the public on computers.</td>
</tr>
<tr>
<td></td>
<td>Dependency of the public on mobile devices (e.g. smartphones).</td>
</tr>
<tr>
<td></td>
<td>Criminal awareness of the success of hacking.</td>
</tr>
<tr>
<td></td>
<td>Ease of entry into hacking (free books, online tutorials, cheaper bandwidth).</td>
</tr>
</tbody>
</table>

6.5 Any additional comments:

...........................................................................................................................................................................
...........................................................................................................................................................................
...........................................................................................................................................................................
...........................................................................................................................................................................

7. Your views on responses to hacking

7.1 Indicate the extent to which the responses below address the risk of hacking in your organisation. Select or click one option in each row below:

<table>
<thead>
<tr>
<th>1 = To a large extent</th>
<th>2 = To a moderate extent</th>
<th>3 = To a small extent</th>
<th>4 = Not at all</th>
<th>5 = Do not know</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate governance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal control</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT governance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Governance frameworks, such as CobiT</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Applying service and quality management, such as ITIL</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information security management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software development practices</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ethical hacking</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security technologies, such as firewalls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

7.2 Indicate how effective each of the responses to hacking is in your organisation. Select or click one option in each row below:

<table>
<thead>
<tr>
<th>1 = To a large extent</th>
<th>2 = To a moderate extent</th>
<th>3 = To a small extent</th>
<th>4 = Not at all</th>
<th>5 = Do not know</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate governance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Annexure D

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal control</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>IT governance</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Governance frameworks, such as CobiT</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Applying service and quality management, such as ITIL</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Information security management</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Software development practices</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Ethical hacking</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Security technologies, such as firewalls</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

7.3 Any additional comments:

……………………………………………………………………………………………………………
……………………………………………………………………………………………………………
……………………………………………………………………………………………………………
……………………………………………………………………………………………………………
……………………………………………………………………………………………………………

8. Ethical hacking

8.1 Ethical hacking can be defined as the act of an ethical hacker breaking into an organisation’s systems by using the same techniques as hackers would, however with explicit authorisation, in an effort to test the organisation's network and system defences. Indicate the extent to which you agree with the following question:

1 = To a large extent
2 = To a moderate extent
3 = To a small extent
4 = Not at all

Do you think that ethical hacking is an effective response to hacking in the bank? ☐ ☐ ☐ ☐ ☐

8.2 Has your organisation ever made use of ethical hacking in the bank? Click or check one answer below.

Yes ☐ No ☐

8.3 Rank the four disadvantages associated with the use of ethical hacking in your organisation, by writing or typing the numbers 1 (most important) to 4 (least important) in the column provided. Use the numbers 1 to 4 only once.

| Confidential information could be disclosed during an ethical hacking assignment. | Rank |
| Banking systems may be affected by ethical hacking activity. | |
| The success of ethical hacking assignments depends on the skills level of the ethical hacker. | |
| Ethical hacking results might be ambiguous and complex to remediate. | |
8.4 Rank the four advantages associated with the use of ethical hacking in your organisation, by writing or typing the numbers 1 (most important) to 4 (least important) in the column provided. Use the numbers 1 to 4 only once.

<table>
<thead>
<tr>
<th>Advantage</th>
<th>Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test the effectiveness of internal control against hacker attacks.</td>
<td></td>
</tr>
<tr>
<td>Persuade management of the threat of hacking.</td>
<td></td>
</tr>
<tr>
<td>Identify and remediate information security and software vulnerabilities.</td>
<td></td>
</tr>
<tr>
<td>Avert potential reputational losses due to hacker attacks.</td>
<td></td>
</tr>
</tbody>
</table>

8.5 Do you follow any unique recruitment practices when employing an ethical hacker? Click or check one answer below.

Yes ☐ No ☐

8.6 Any additional comments:

........................................................................................................................................................................
........................................................................................................................................................................
........................................................................................................................................................................
........................................................................................................................................................................

9. Personal information

9.1 What is your highest qualification?

........................................................................................................................................................................

9.2 What is your highest IT specific qualification?

........................................................................................................................................................................

9.3 How many years' experience do you have in IT governance?

........................................................................................................................................................................

9.4 Any additional comments:

........................................................................................................................................................................
........................................................................................................................................................................
........................................................................................................................................................................
........................................................................................................................................................................
Thank you for participating!