CHAPTER ONE:
GENERAL ORIENTATION TO THE DISSERTATION

1.1 Structure of chapter

"It is insufficient to protect ourselves with laws, we need to protect ourselves with mathematics."[1]

This dissertation will convince the reader, not only of the fictitiousness of this statement, but also of the inherent danger attached to making such a statement.

The dissertation concerns itself with the legal implications of information security governance. As a general point of departure clarity and certainty will have to be obtained regarding the following fundamental issues:

(i) What is information security governance?
(ii) Why is it important? and
(iii) Who is responsible for it?

Once these three initial questions have been answered the dissertation will provide practical, pragmatic advice on:

(i) How to implement information security;
(ii) How to measure the performance of information security within the organisation; and
(iii) How to escape liability for failed information security.

[1] Schneier *Secrets and Lies* (2000) xi made this comment in 1995. He did however recognise and correct his mistake five years later in his book *Secrets and Lies* (2000).

The exposition of this dissertation is therefor aimed at education, while simultaneously empowering those responsible for information security governance, on what this discipline entails, why they should concern themselves with this discipline, and what their legal obligation under this discipline is.

Outline of chapter:

The legal implications of information security governance centers around the following five questions:

(i) What is information security governance?
(ii) Why is information security governance important?
(iii) Who should be concerned with information security governance?
(iv) How is information security governance implemented within the organisation? and
(v) What are the legal consequences of non-compliance with information security governance?

Part 2: will provide the reader with a general introduction to the legal implications of information security governance, before addressing the five questions identified above;

Part 3: will contain the problem statement of the dissertation;

Part 4: will identify the objective of the dissertation; and

Part 5: will give a brief overview of the dissertation.

1.2 Introduction to the legal implications of information security governance

Background to information security governance

Since most organisations have moved from the physical world into cyberspace, information security governance has become pivotal to this new realm. Cyberspace represents a two-edged sword: by making use of electronic communication systems,[2] such as e-mail, [3] faxes and the world-wide-web, [4] organisations are able to gain access to an unlimited pool of customers and unprecedented array of opportunities, while simultaneously exposing themselves to a multitude of new risks, threats and vulnerabilities never envisaged before.

This dissertation concerns itself with the legal implications of information security governance. Arguably the most important implication would be that non-compliance with this discipline may result in legal liability. This is clearly outlined in the King II Report on Corporate Governance[5] which places, in no uncertain terms, the ultimate responsibility for information security firmly in the hands of the board of directors.[6] This is furthermore in line with the approach taken by the international community to information security. The international community classifies the responsibility of taking adequate steps to secure the organisation's information assets under a director's fiduciary duty of care and skill/due diligence. Consequently, failed information security may

---

2 Section 1 of the Electronic Communications and Transactions Act 25 of 2002 defines electronic communications as: "…a communication by means of a data message."

3 Section 1 of the Electronic Communications and Transactions Act 25 of 2002 defines e-mail as: "…electronic mail, a data message used or intended to be used as a mail message between the originator and addressee in an electronic communication."

4 Section 1 of the Electronic Communications and Transactions Act 25 of 2002 defines the World Wide Web as: "…an information browsing framework that allows a user to locate and access information stored on a remote computer and to follow reference from one computer to related information on another computer."

5 King Committee *King II Report on Corporate Governance 2002* (2002).

6 Section 1 of the Companies Act 61 of 1973 defines the term "director" as to include: "…any person occupying the position of director or alternate director of a company, by whatever name he may be designated." Confusion may arise as the term "directors" is sometimes used in literature intercurrently to refer to the plural of an individual director, and to the board of directors.

directly be equated to failure to comply with the duty of care and skill, which may ultimately result in personal liability.

The Electronic Communications and Transactions Act[7] (henceforth ECT Act) also addresses specific security issues, such as digital signatures[8] by making it compulsory in certain cases. It should however be realised that there exists a very fragile interrelationship between privacy, trust and security, with the former two concepts indirectly impacting on information security. Therefor organisations will have to take note of the ECT Act,[9] and specifically those chapters relating to technical security (digital signatures); trust (cryptography[10] and authentication[11]); and privacy (protection of

---

7 25 of 2002.

8 Section 1 of the Electronic Communications and Transactions Act 25 of 2002 defines an electronic signature as: "…data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature." The act goes on to define an advanced electronic signature as: "…an electronic signature which results from a process which has been accredited by the Authority as provided for in section 37." Section 13 of this act deals specifically with signatures and the legal consequences attached to them.

9 25 of 2002.

10 Section 1 of the Electronic Communications and Transactions Act 25 of 2002 defines a cryptography product as: "… any product that makes use of cryptographic techniques and is used by a sender or recipient of data messages for the purpose of ensuring –

(a) that such data can be accessed only by relevant persons;
(b) the authenticity of the data;
(c) the integrity of the data; or
(d) that the source of the data can be correctly ascertained."

The act goes further to define a cryptography service as: "… any service which is provided to a sender or a recipient of a data message, and which is designed to facilitate the use of cryptographic techniques for the purpose of ensuring –

(a) that such data or data message can be accessed or can be put into an intelligible form only by certain persons;
(b) that the authenticity or integrity of such data message is capable of being ascertained;
(c) the integrity of the data or data message; or
(d) that the source of the data or data message can be correctly ascertained."

Chapter five of the ECT act deals specifically with cryptography providers.

11 Chapter four of the Electronic Communications and Transactions Act 25 of 2002 deals specifically with authentication providers, procedures, and requirements for accreditation of authentication products and services.

personal information[12] and consumer protection[13]), as a security breach in any one of these domains may ultimately result in legal liability. [14]

Therefor organisations, and specifically those people entrusted with the governance of the organisation, are being places under increased pressure through new laws, regulations and standards to ensure that they have taken the necessary steps to secure the organisation's information assets.[15]

As stated earlier legal implications of information security governance centers around five main questions. Therefor when wanting to gain insight into what the discipline information security governance entails, clarity and certainty must be obtained regarding the following questions: (i) what is information security governance? (ii) why is it important? (iii) who should be concerned with it? (iv) how is it implemented within the organisation? and (v) what are the legal consequences for non-compliance with this discipline?

(i) What is information security governance?

Information security is concerned with "the protection of valuable assets against loss, misuse, disclosure or damage."[16] Governance, in turn, concerns itself with the way in which the organisation is being managed. Therefor the amalgamation of these two concepts (information security + governance) result in the genesis of a new governance discipline namely, information security governance.

---

12 Chapter eight of the Electronic Communications and Transactions Act 25 of 2002 regulates the protection of personal information.

13 Consumer protection is specifically dealt with in chapter seven of the Electronic Communications and Transactions Act 25 of 2002.

14 Cazemier, Overbeek and Peters *Security Management* (2001) 9 defines an information security incident/breach as: "…events that can cause damage to confidentiality, integrity or availability of information or information processing. They materialize as accidents or deliberate acts."

15 See Annexure A for a comprehensive list of national and international information security legislation, regulations and standards.

16 IT Governance Institute "Information security governance" (last visited 24 July 2002) http://IT governance.org 8.

Information security governance is concerned with how those people entrusted with the governance of an entity will consider and administer information security in their supervision, monitoring, controlling and directing of that entity.

Therefor, information security governance is a collective noun used to describe the business and legal impact, considerations and consequences embedded in information security-related issues.

(ii) Why is information security governance important?

Information[17] has always been one of the most important assets over which organisations possessed. However, with the advent of the information age, the importance of these information assets have increased exponentially, as all electronic transactions inevitably involve information being created, processed, stored, transmitted, used or communicated. Consequently, "…as dependence on information systems increase, so too does the criticality of information security, bringing with it the need for effective information security governance."[18]

Notwithstanding this, the best way of illustrating and convincing organisations of the need for, and importance of information security governance, is still to be found in focussing on the benefits derived from the effective implementation of this discipline.

---

17 The terminology "data" and "information" are often used interchangeably. This is however incorrect. The term "data" refers to "…facts and figures that are relatively meaningless to the user…." or "…a series of bits…"; whereas the term "information" refers to "…processed data, or meaningful data …comprehensible to someone it becomes information which can be used by a process performing an action on behalf of the user." Roberts *Computer Security Policy* (1990) 2. The Electronic Communications and Transactions Act 25 of 2002 neglects to define the term "information," but section 1 of the Act does define the term "data" as "…electronic representation of information in any form."

18 Roberts *Computer Security Policy* (1990) 8.

As will be discussed in later chapters numerous benefits are attached to information security governance, ranging from strategic alignment, value delivery, risk management, to performance measurement. However, arguably one of the most important benefits derived from this discipline is legal compliance with information security legislation, regulations and standards.

(iii) Who should be concerned with information security governance?

Information security governance is a topic of immediate concern for all companies making use of electronic communication media. Therefore, the scope of application of this discipline is not only limited to companies with websites, but applies to all companies that make use of online facilities. As soon as a company is connected it is vulnerable and susceptible to attacks, therefor interconnectivity should go hand-in-hand with information security governance.

This dissertation is specifically aimed at addressing the legal implications of information security governance for public[19] and private[20] companies. It should however be kept in mind that there are inherent differences between private and public companies.[21] This objective is achieved by differentiating between two groups of role-players within the organisation itself, namely primary role-players and secondary role-players.

---

19 A private company is a company in which at least two persons come together for a lawful purpose. Characteristics of a private company are the following:

(i) The name of a private company must end with "(Proprietary) Limited";
(ii) Restriction on free transferability. The right to transfer shares are restricted;
(iii) Limitation on membership. The number of members of a private company are limited to 50;
(iv) Financial statements do not have to be made public; and
(v) An invitation to the public to subscribe for shares in the private company is prohibited.

20 In a public company at least seven people come together for a lawful purpose.
Characteristics of a public company:

(i) The name ends with the word "Limited";
(ii) There is no restrictions on the transferability of shares;
(iii) Membership in the public company is open to the public, and no limitation, with regards to numbers are placed on it;
(iv) Great emphasis is placed on disclosure and certain financial statements must be disclosed to the public.

21 The main differences between a private and a public company as summarised in Cilliers, Benade, Henning, Du Plessis, Delport, De Koker and Pretorius *Corporate Law* (2000) 41-42 are:

(i) "The last word in the name of a private company must end with "(Proprietary) Limited"; whereas in the case of a public company only the word "Limited" must appear.
(ii) A private company, unlike a public company, need not lodge any financial statements with the Registrar;
(iii) Unless the articles provides otherwise, a member of a private company may not appoint more than one proxy;
(iv) Unless the articles provide otherwise, the quorum for a general meeting of a private company is two members entitled to vote who are present, or if a member is a body corporate, represented. In the case of a private company with only one member, the quorum is one. The quorum in the case of a public company is three;
(v) The voting rights of a public company are proportional to the number of shares held. The voting rights attached to shares in a private company can be regulated more freely in the articles;
(vi) A private company must have at least one director, while a public company must have at least two;
(vii) A director who held office for life in a private company on 13 June 1949 cannot be removed from office;
(viii) A private company must have at least one member, while at least seven members are required for a public company; and
(ix) The auditor of a private company may also be the secretary or bookkeeper of the company in certain circumstances. This is strictly prohibited in public companies."

Primary role-players would include the board of directors and top management.[22] Information security governance should be a major concern for these two entities as they may incur personal liability for failed information security. Ultimate therefor, responsibility for information security resides in the board of directors, and top management is in turn answerable to the board on this issue. It should however be kept in mind that it can not be expected of the board to be involved in the day-to-day development and implementation of information security initiatives. Consequently, the board is allowed to delegate certain functions for the development and implementation of this discipline to designated employees. These designated employees will constitute the secondary role-players. It would therefor be expected of them to develop and implement information security within the organisation.

Secondary role-players include, but are not limited to:

(a) IT manager;
(b) IT service manager;
(c) Security coordinator;
(d) Department manager
(e) Systems and applications administrator;
(f) IT service level manager;
(g) Risk and security manager;
(h) Business information manager;
(i) Business manager;
(j) Procurement manager;
(k) Supplier managers;
(l) Account managers;
(m) Auditors; and
(n) Consultants.

[22] The South African Institute of Chartered Accountants defines management as follows: "…management comprises of officers and others who also performs senior managerial functions." Section 1 of the Companies Act 61 of 1973 defines the term "manager" as: "…any person who is a principal executive officer of the company for the time being, by whatever name he may be designated and whether or not he is a director."

(iv) How is information security governance implemented?

Information security governance is implemented within the organisation by combining three components of information security namely, physical security, technological security, and procedural security. The development, execution, monitoring and evaluation of these components will be of pivotal importance to the success of the information security governance discipline. Furthermore, the better these components fit together, the greater the benefits that will be derived from this discipline.

(v) Consequences of non-compliance?

The final and perhaps the most important question that must be answered is: "if information security fails, who is to blame?"

A legal means must therefor be found to hold those people responsible for information security accountable. The answer to this question is found in the common law, and more specifically the fiduciary duty of care and skill. [23] Therefor, within the information security domain, a director's duty of care and skill, will ultimately form the basis on which a plaintiff will be able to hold a director personally liable for failed information security.

[23] The reader should keep in mind that the duty of diligence in American company law may be equated to the duty of care and skill found in other jurisdictions. Bowden, Lane and Martin *Triple Bottom Line Risk Management* (2001) 116-117 define due diligence as: "(t)he essence of a due diligence defense is the establishment and implementation of procedures designed to ensure that managers, employees, agents, and third-party contractors comply with applicable laws, license conditions, and industry standards and prevent the occurrence of adverse impacts." Due diligence defense requires proof that risks were identified and addressed. What action was taken, by whom, when, what was the outcome; and what follow-up action, monitoring, and review were undertaken?"

1.3 Problem statement

Problem identification: Organisations doing business in the information age are operating in a business atmosphere that is fraught with risks, threats and vulnerabilities constantly in flux. All risks, threats and vulnerabilities have as their first and foremost objective to compromise the information assets of the organisation.

The **solution** to this **problem** comes in the form of information security governance which enables the organisation to reduce risks to an acceptable level.

Quandary: Inability of directors and top management alike to apply the solution to the problem. Put differently, organisations know what the problem is, they know what the solution to the problem is, but they are unable to apply the solution to the problem.

In practical terms this would mean that those who are responsible for the governance and management of the organisation, therefor the board of directors and top management: (i) do not know what the solution (information security governance) entails; and/or (ii) do not know how to apply the solution to the problem.

This problem is as a direct result of directors and managers inability to realise, understand and appreciate:

(i) That information security is a business issue, and not a technology issue;
(ii) The value information security holds for the organisation;
(iii) The threats facing the information assets of the organisation;
(iv) How these threats can be reduced to an acceptable level; and
(v) What resources are needed to reduce threats to information security.

However, without a comprehensive understanding of the above directors and top management will be unable to provide managerial direction for information security. Consequently, it appears that most organisations lack direction on information security.

Even if information security does exist to some extend in the organisation, one will often find:

(i) Lack of top management support and commitment for the discipline;

(ii) Misalignment between objectives, mission and goals of information security and that of the organisation as a whole;

(iii) General absence, or lack of an awareness and training program and other critical success factors such as information security policies, standards, procedures and guidelines;

(iv) Insufficient funding for information security initiatives; and

(v) Increase in security incidents with a re-active approach being taken by the organisation.

If the board understands the legal implications of information security governance they will be able to unite the problem with its solution, as they would have gained insight into what the discipline information security governance entails, and how it is applied/implemented in practice.

1.4 Objectives of dissertation

The aim of this dissertation is two-fold:

(i) Enabling directors and top management to gain a better understanding of the legal implications of information security governance by addressing the problems as identified above; and

(ii) Empowering directors and top management by providing them with an infrastructure to:

- Develop information security policies, standards, procedures and guidelines, as well as information security audit checklists and control questionnaires;

- Discover information security best practices from other organisations;
- Improve overall information security within the organisation; and
- Comply with internationally acceptable information security standards.

If they comply with the recommendations made in this dissertation they will have gone a long way in:

- Ensuring that their organisation's information assets are protected from external and internal threats, risks, and vulnerabilities;
- Ensuring risks are reduced to an acceptable level;
- Ensuring a sufficient information security culture is fostered within the organisation;
- Ensuring protection is accomplished in a manner consistent with business requirements; and
- Ensuring that they have complied with their fiduciary duty of due diligence.

1.5 Overview of dissertation

Framework of dissertation:[24]

The following questions will be addressed in the dissertation:

[24] The framework of this dissertation is based on a framework as discussed in CIO "Creating a culture of security" (last visited 28 August 2003) http://www.cio.com S2-S3.

Each chapter will identify one or more problematic issues that must be addresses:

Chapter One: provides a general orientation to the dissertation by providing the reader with an introduction to the legal implications of information security governance. Five questions are identified as forming the spill around which information security governance revolves, namely: (i) what is information security governance? (ii) why is it important? (iii) who should be concerned with it? (iv) how is it implemented within the organisation? and (v) what are the legal consequences for non-compliance with this discipline? The objective of the dissertation is furthermore identified, before giving a brief overview of the entire dissertation.

Chapter Two: provides the reader with a general introduction to the art and science of information security. As a point of departure certain preliminary perceptions organisations have about information security are discussed before moving on to the semantics of information security. The researcher identifies six pillars of information security that has as its first and foremost objectives the delivery of an adequate and sustainable level of security within the organisation.

In the pursuit of information security the following sentiments about this discipline must be kept in mind. Firstly, that information security is a process, not a product. As a process it has many components that should be used in conjunction with one another. The better these components fit together, the more efficiently and effectively information security will be used within the organisation. This chapter will emphasise the fact that information security involves more than erecting physical and electronic barriers. Information security is a holistic discipline of which no one component may be ignored. Therefor, proper governance of this discipline demands the management of every component thereof. Consequently, the physical, technological, as well as non-technological/procedural aspects of information security must be addressed.

Secondly, information security is a business problem, not a technology one. Increasingly the legal and business aspects of information security are going to receive attention.

Providing information security means that legal consideration must be given to the way in which information is created, processed, stored, transmitted, used and communicated; who has access to it; what they will be able to do with it; how long they will be able to have access; and who has the authority to change access and how.

Lastly, information security is a chain; it's only as secure as its weakest link. It is a common known fact that today's most secure system will be vulnerable tomorrow. In knowing and acknowledging that the organisation is vulnerable, therein lies the key to information security.

These three sentiments will be reiterated throughout this dissertation as they form the core of information security.

This chapter therefor presents a brief survey of some of the basic concepts underlying the discipline information security. Keep in mind that no attempt is made to give a comprehensive understanding of information security as it is a very broad subject-matter with an incredible amount of methodology and practices.

Chapter Three: reminds the reader that the concept of governance is not foreign to corporate South Africa. Organisations have been grappling with this concept since 1994 when the King report on Corporate Governance codified corporate governance into South African law. However, with the advent of the information age and associated information technology [25] developments, a new medium was introduced that needed to be governed namely, cyberspace. Consequently, a new governance discipline information security governance emerged, to address concerns relating to interconnectivity, the ease with which information may be accessed and transmitted, combined with the organisation's dependence on its information resources.

---

[25] Boar *The Art of Strategic Planning for Information Technology* (2001) 2 defines information technology as: "(t)he preparation, collection, transport, retrieval, storage, access, presentation, and transformation of information in all its forms (voice, graphics, text, video, and image). Information movement can take place between humans, humans and machines, and/or between machines. Information management ensures the proper selection, deployment, administration, operation, maintenance, and evolution of the IT assets consistent with organisational goals and objectives."

This chapter therefor identifies information security governance as a specie of the overall governance concept and will accentuate the board and management's responsibility to extend the governance discipline to include information security governance. It is expected of the board and top management to make information security governance an integral part of their organisation as a whole.

Chapter Four: concerns itself with information security leadership, and more specifically those entities responsible for the development and implementation of information security governance within the organisation, namely the board of directors and top management. These two entities are faced with a wide variety of complex issues in the information age. One of which being that many directors have a vast knowledge and expertise of a bricks-and-mortar approach to organisations, as they were educated on the governance of a company before information technology became the core of every organisation's existence. Directors need a change in mindset from governance of brick-and-mortar organisation, to click-and-mortar organisation.

It is furthermore of the utmost importance that directors start making a conscious effort to become informed about the discipline information security, as information security is viewed as a critical board task. Ultimately the board and top management will have to answer the question if they think their organisation's information assets are secure, or if they know that it is secure. The answer to this question will have far reaching legal implications for them.

Chapter Five: will attempt to capture the illusive value of information security. It is increasingly expected of managers and executives alike to provide stakeholders and shareholders with hard concrete facts on the performance of information security within the organisation. Crucial decisions such as resource allocation, investment, re-investment decisions and even project authorisation will depend on information security's ability not only to meet expectations, but also to exceed them.

Two of the biggest problems experienced when attempting to measure the performance of information security is firstly, that the benefits delivered by information security are of an intangible nature, and therefor inherently hard to place a monetary value on; and secondly, information security is not used solely in one unit, department or application of which the performance may be measured. Information security forms an integral part of the organisation as a whole, and cannot be resected from it without resulting in an all but complete collapse of the organisation.

The ultimate aim of this chapter is to convince directors and top management of the business impact information security has on the bottom line. The business case for information security governance will be made in two ways. Firstly, the value of information security will be illustrated through performance measurement, and specifically the balanced scorecard, which is able to justify cost and measure the performance of the intangible benefits offered by this discipline. Secondly, to indicate how information security acts as a business enabler attention must be focused on strategic alignment to demonstrate how information security mission, goals and objectives, if in harmony/aligned with the overall organisational mission, goals and objectives, will function as a powerful tool to enhance economic efficiency, boost productivity growth, and obtain a sustainable competitive advantage.

Chapter Six: has as its aim to provide directors and top management with a methodology in the form of a usable framework for the implementation of information security governance within the organisation. The framework takes a life cycle approach to reflect the frenetic real world of information security, where the furious pace of technological changes presents both numerous opportunities and increased risks.

Implementation is embodied in a multitude of layers/phases. Each phase will act as a continuation of the previous phase and a predecessor of the next. The implementation process will address numerous issues, including (i) determining the **radius of risk** to information security within the organisation by making use of an effective **risk management** process. During this risk management process the following questions will

be addressed: (a) What is the organisation trying to protect? (b) From who are you trying to protect it? (c) What will be the impact if the risk materialises? and (d) What safeguards or control measures should be implemented to reduce the risk to an acceptable level? Risk management comprises of two components, namely risk assessment and risk mitigation. During the risk assessment stage three variables are identified, namely the threat agent, the threat motive, and the impact if the threat materialises. Therefor risk assessment requires of directors and top managers to understand the risks facing the organisation before they can move on to the second component, namely risk mitigation in which safeguards and countermeasures will be selected and deployed in order to make an unacceptable risk acceptable. When selecting appropriate countermeasures consideration must be given to cost-benefit analysis; (ii) the development and implementation of **information security policies, standards, procedures and guidelines**, to ensure information security is deployed and enforced in a consistent manner throughout the organisation. This phase is said to be the foundation of any information security initiative; (iii) raising the **awareness of information security** issues amongst employees by educating them on why the need for information security exist, what is expected of them, and what consequences will ensue of they do not adhere to the proposed policies, standards and procedures is crucial. Event the best formulated information security policy will sit dormant on a shelf if those people who are expected to comply with it are not made aware thereof. Therefor an effective organisation-wide, ongoing awareness and training program is crucial to the success of any information security governance discipline. "Awareness implies understanding the risk;"[26] (iv) **maintaining and monitoring** information security is just as important as implementing it in the first place. It might even be harder to achieve, as maintenance and monitoring requires renewed commitment to information security efforts on a daily basis.

It will be evident from this chapter that the implementation of information security is a complicated, time-consuming endeavor which is neither straightforward, nor inexpensive, moreover, it raises significant legal and managerial issues. Keep in mind that

[26] Hunter *Information Security: Raising Awareness* (2000) 5.

organisations no longer have a choice between implement information security governance, or refraining from doing so. It is mandatory, not optional.

Chapter Seven: discusses legal liability for information security, and provides several penetrative law pointers on how to limit liability, ranging from continuous security improvements to compliance with internationally acceptable standards on information security.

Unfortunately, directors and top management's perspective of information security is based on assumptions. They generally assume that their information assets are secure and that appropriate security measures are in place. These assumptions are however very dangerous, as it can ultimately lead to directors being held personally liable for not taking reasonable steps to secure the information assets.

This chapter therefor highlights the interplay between law and information security. Law and technology are strange bedfellows, and in general we find that the law, specifically relating to information security issues, lags far behind. It may therefor be surprising for some to discover that a director's liability for not securing the information assets of his organisation is not to be found in some piece of newly enacted legislation, but rather in the long-established common law principle of duty of care and skill.

The only question that a court will ask once a security incident/breach has occurred within the organisation, is whether or not the director took reasonable steps to secure its information assets, therefor did he fulfill his duty of due diligence? This question will be asked irrespective of the type of security incident that has occurred, be it theft of confidential information, industrial espionage or hacking, they will all fall under this one duty.

The chapter will furthermore illustrate through case law that the duty of care and skill may be equated to the shift in the pendulum that tends to oscillate between pro-plaintiff and pro-defendant attitudes over time. In the 19th century and early parts of the 20th

century, a relatively low standard of care and skill was required of directors. At present however, directors must be mindful of the fact that the duty of care and skill is being applied more strictly.

Chapter Eight: contains findings and recommendations that will aid the board in discharging the multitude of onerous responsibilities and duties information security governance place on them. It is concludes that information security may be equated to a seemingly endless chess match, wherein both sides respond to the moves made by his opponent.[27] Therefor, organisations will continue to respond to the increased capabilities of his opponent (threat agent), by the implementation of safeguards and control measures, while the opponent will view these control measures as a challenge, and will look for a new way in. [28] It is therefor incumbent on those who are in a position of authority to take up the challenge of information security governance. Not only to protect the organisation as a whole, but also to escape personal liability for non-compliance with their duty of due diligence.

"There are expected to be 502.5-million online users in 2003 and it takes only one to invade your perimeter, destroy your brand and hurt your revenue."[29] Consequently, if organisations only protect themselves with mathematics, and fail to bring other components of the discipline information security governance into the equation, the organisation, and those responsible for the governance of the organisation, will sooner rather than later end up in court.

---

27 Tipton and Krause *Information Security Management Handbook* Vol 2 (2001) 145.

28 ibid.

29 Boespflug, Neal and Crowe "Secure your systems now: Just one hacker can wreck your business" (last visited 18 April 2002) http://www.itweb.co.za 5.