CHAPTER TWO: INFORMATION SECURITY PRINCIPLES

2.1 Structure of chapter

The purpose of this chapter is to provide directors and top management with a brief overview of the fundamental principles inherent to the art and science of information security. It is not an attempt to educate these entities on the technical aspects thereof, but rather a discussion of the most important aspects underlying this discipline.

The objective of this chapter is therefor to address three principal questions, namely:

(i) What is information security?

(ii) Why is information security important? and

(iii) Who are the primary and secondary role-players in the information security domain, and what are their functions?

Outline of chapter:

Part 2: will give a brief overview of perceptions organisations have about information security;

Part 3: will define what the concept information security entails;

Part 4: will identify the key drivers behind the increased awareness of information security;

Part 5: will describe some of the benefits organisations will derive from the effective implementation of information security;

Part 6: will attempt to prove that information security is a business issue and not a technology one by identifying key role-players in the information security discipline;

Part 7: will discuss the semantics of information security by focussing on this discipline's components, pillars and models; and

Part 8: will address the controversial issues of regulating information security.

2.2 Preliminary Perceptions

As a point of departure to any discussion on information security it is instrumental to observe certain preliminary perceptions, or rather misconceptions, organisations have regarding this discipline:

(i) Firstly, organisations tend to throw money at the information security problem with the belief that they can buy information security.[1] However, information security "does not exist in a box by itself."[2] Consequently, organisations will have to be concerned with information security "in all its forms"[3];

(ii) Secondly, organisations would like to believe that for every security problem there is a technological solution. They therefor believe that technical products will solve all their information security problems. Consequently, organisations take a piecemeal approach to information security, placing a wholly inappropriate degree of reliance on technology. The problem however lies therein that if security is conceived as principally a technological problem, the focus is drawn away from the other two equally important components of information security, namely physical security and non-technological/procedural security. It must be realised that information security is a holistic discipline of which no one component may be ignored;[4]

(iii) Thirdly, organisations believe that because they do not do anything that makes them a target, they are safe.[5] However, organisations need to realise that they do

---

1 Jenkins "Organizational IT security theory and practices: and never the twain shall meet?" (last visited 27 February 2003) http://www.sans.org/rr/securitybasics/IT_sec2.php 6.

2 Sommer "How to buy information security" (last visited 24 July 2003) http://www.virtualcity.co.uk.hottobuy.htm 1.

3 (n 2) 2.

4 Unknown "Cyber war imminent, mobilise your defenses – Unisys Africa chief" (last visited 18 February 2002) http://www.computingsa.co.za/compaarchive/2001/09/10/communications/sec01.htm 1.

5 Marsh "Myths managers believe about security" (last visited 27 February 2003) http://www.sans.org/rr/start/myths.php 4.

not have to do anything, or be someone before falling victim to an attack. Acknowledge the fact that attackers do not need a reason to attack you; [6] and

(iv) Finally, organisations believe that because they have not yet fallen victim to an attack, they must have effective security measures in place to adequately protect their information assets. There is however a flaw in their reasoning, as most organisations do not audit changes in their systems and/or application. Therefor, they would not know if something has been changed or modified. Even those organisations that feel confident that they would be able to detect a security breach or incident must answer two questions:

(a) When will the organisation be able to detect the attack? During the attack, afterwards, and how long afterwards? [7] and

(b) Could the organisation measure the impact of the attack? [8]

The mere fact that an organisation has not yet been broken into does not mean that that organisation has good security, it simply means that it has been lucky thus far. [9]

6 ibid.
7 ibid.
8 ibid.
9 ibid.

2.3 Defining information security[10]

Zedner[11] correctly remarks that:

> "Security is a slippery concept. Its meanings are multiple and without clarity about which meaning is intended, exactly what is being provided and consumed, sold and bought, promised or sought remains obscure. Security is both a state of being and a means to an end." [12]

For purposes of this dissertation information security is defined as:

> "Security relates to the protection of valuable assets against loss, misuse, disclosure or damage.
>
> **(i)** **Valuable assets** are information recorded on, processed by, stored in, shared by, transmitted or retrieved from an electronic medium;
>
> **(ii)** **Information** must be protected against harm and threats leading to different kinds of vulnerabilities such as loss, inaccessibility, alteration and wrongful disclosure;
>
> **(iii)** **Threats** would include, but are not limited to errors and omissions, fraud, accidents and intentional damage; and
>
> **(iv)** **Protection** arises from layers of technological and non-technological safeguards, such as physical security measures, background checks, user identifiers, passwords, smart cards, biometrics and firewalls. Safeguards

---

10 Various attempts have been made to define information security. Some of the more auspicious definitions are depicted below. The Security and Privacy Research Center defines information security as: "…the process of protecting data from accidental or intentional misuse by persons inside or outside the organisation" Scalet "Security and privacy research center glossary" (last visited 18 November 2002) 2. KPMG "Global information security survey" (last visited 18 November 2002) http://www.kpmg.co.uk 3 defines information security as: "…the practice, procedures and technology which ensures that information is safeguarded from unauthorised access, modification or accidental change, and is readily available to authorised users on request." The National Security Agency's (NSA) glossary for security and intrusion detection defines information security as: "(t)he result of any system of policies and/or procedures for identifying, controlling, and protecting from unauthorised disclosure, information whose protection is authorised by executive order or statute" SANS "NSA glossary of terms used in security and intrusion detection" (last visited 27 February 2003) http://www.sans.org/resources/glossary.php 7.

11 "The concept of security: an agenda for comparative analysis" (March 2003) *Legal Studies* 154.

12 The terms security and privacy are often used interchangeably. What the customer views as privacy the organisation classifies as security. It should however be guarded against confusing these two terms, as they have very different legal meanings and consequences embedded in them. The reader must be mindful of the fact that this dissertation will concern itself with security and not privacy.

should address both threats and vulnerabilities in a balanced manner" [13] (own emphasis).

Consequently, information security has as its **objective**:

(i) "The protection of information assets of the organisation while being transmitted, used, stored, or processed;
(ii) Enabling the organisation to take full advantage of the information by unleashing the benefits associated with the information;
(iii) Gaining a sustainable competitive advantage;
(iv) Enabling and supporting the business in achieving set goals, missions and objectives; and
(v) Aligning business goals and objectives."[14]

2.4 Key drivers of information security

The importance of information security is best captured by the following citation: "information is power, power is information, and ignorance is bliss."[15] Throughout this dissertation the researcher will reiterate the point that information is one of the most valuable assets over which an organisation may possess.[16] Without it only a few processes are able to function and operate as intended. [17] Consequently, it follows that anything that threatens the information asset of the organisation will directly endanger the performance of that organisation. [18]

The increased focus on information security may be ascribed to the following factors:

(i) **Widespread use** of technology;
(ii) **Complexity** associated, not only with information technology (henceforth IT), but also the security needed to protect information assets, has increased

---

13 IT Governance Institute "Information security governance" (last visited 28 June 2002) http://www.ITgovernance.org 8-9.
14 Warman *Computer Security within Organizations* (1993) 71.
15 Heske "Security 2001: As strong as the weakest link in the chain" (last visited 18 February 2002) http://www.computingsa.co.za/compsaarchive/2001/01/29/feature/fea01.htm 1.
16 Cazemier, Overbeek and Peters *Security Management* (2001) 7.
17 ibid.
18 ibid.

exponentially.[19] Keep in mind that complexity is a hacker's friend, the more lines and codes there are, the more likely it is that a vulnerability will exist;[20]

(iii) **Interconnectivity**. In the past organisations had a stand-alone mainframe, which they needed to secure. At present however, "everything is connected to everything else"; [21]

(iv) **Growing potential for misuse.** Organisations are dealing with an enemy that is increasing not only in numbers, but also in intelligence; [22]

(v) **The rapid rate at which new technology is developing and old technology becomes obsolete,** makes it increasingly difficult for organisations to keep up with the latest security safeguards and control measures. It is difficult to keep abreast of the changing tide of information security;

(vi) Increased **mobility** of the workforce;[23]

(vii) **Increasing number of vulnerabilities in security products and technology** are raising organisation's awareness, not only of their own evanescence, but also of the fact that technology alone can not adequately secure the organisation's information assets;[24] and

(viii) The **threat of legal liability** for failure to adequately secure the organisation's information assets is on the increase.[25] The board may be judged irresponsible if they did not take the necessary steps to adequately secure the organisation's information assets.

---

19 Symantec "The value of information security" (last visited 24 July 2002) http://www.symantec.com 5.

20 Unknown "Keeping the enemy at bay" (last visited 18 February 2002) http://www.computingsa.co.za/compsaarchive/2002/01/28/communications/sec04.htm 1.

21 ibid.

22 (n 15) 3.

23 Through laptops, Personal Digital Assistants (PDAs) and WAP-enabled cell phones, employees are no longer restricted to the office when conducting business. Greater mobility increases the speed and flexibility with which tasks are performed, but with this greater mobility comes greater security concerns. Planting "The costs of breaches to information security are almost impossible to quantify" (last visited 4 July 2002) http://www.futurecompany.co.za/cgi-bin/pp-print.pl 2.

24 Rasmussen "IT trends 2003: information security standards, regulations and legislation" (last visited 29 May 2003) http://www.csoonline.com/analuyst/report721.html 1.

25 (n 24) 2.

Taking the aforementioned into account it is not surprising that, at present "information security is in a worldwide crisis."[26]

2.5 Benefits inherent to information security

Admittedly, the development and implementation of an effective information security infrastructure within the organisation will be time and resource consuming. However, those organisations that do succeed in implementing information security effectively will experience one or more of the following benefits:

(i) Prevention of incidents such as downtime;[27] intellectual property theft; misuse or destruction of data resources; expenses pertaining to lawsuits; public embarrassment; decrease in stock price; and shareholder confidence;[28]

(ii) Improved business performance;[29]

(iii) An increase in shareholder value;[30]

(iv) Achievement of a sustainable competitive advantage;[31]

(v) Generation of trust and customer confidence;[32]

(vi) Improving and protecting the organisation's reputation;[33]

---

26 Keep in mind that the Y2K crisis appears inconsequential when compared to the imminent information security crisis. The reason for this being that Y2K presented organisations with a static problem. Organisations had the luxury of time and a generous budget to solve the problem. Unfortunately, information security does not present the organisation with a static problem. The information security problem bears a striking resemblance to a living, breathing organism that keeps on evolving. Threat-agents have acknowledged this characteristic of information security, and are making conscious efforts to evolve with this discipline. Unfortunately, organisations have yet to come to this realisation.

27 Downtime may be viewed as being equal to "…work that is never performed and revenues that companies never receive..." Symantec (n 19) 3.

28 (n 19) 12.

29 (n 13) 11.

30 ibid.

31 ibid.

32 ibid.

33 ibid.

(vii) Empowerment of the organisation to conduct business more efficiently, effectively and more profitably in cyberspace as information security functions as a business enabler;[34] and

(viii) Assurance that the information assets over which organisations possess are reliable, easily accessible and taken maximum advantage of, thereby realising its full potential. [35]

2.6 Key role-players in information security

There are certain sentiments about information security that the researcher will reiterate throughout this dissertation merely because of its importance, the first of which being that information security is a business issue and not a technological issue. In order to substantiate this statement attention must be focussed on those people who are involved and have a vested interest in information security, namely:[36]

(i) Organisation itself;

(ii) Employees;[37]

(iii) Customers;[38]

(iv) Suppliers and service providers;[39] and

(v) Stakeholders.[40]

As should be evident from the identification of these role-players, the business side of information security overshadows the technological side thereof completely.

---

34 Information security effectively plays three roles within the organisation. Firstly, there is its tradition role of business supporter, secondly, the now emerging role of business enabler, and finally, the ultimate role of business transformer. Symantec (n 19) 12.

35 Roberts *Computer Security* (1990) 62.

36 Ernst & Young "Global information security survey 2002" (last visited 18 April 2002) http://www.ey.com/global 2.

37 Employee awareness can make or break an organisation's investment in security technology and processes.

38 Customer's availability of systems and business continuity are critical to customer loyalty.

39 Supplier and service providers have employees too, therefor their lack of security awareness can seriously compromise their security, and that of your own organisation.

40 Security threats and incidents can seriously impact on the share price and stakeholder confidence.

Consequently, organisations will no longer be able to focus solely on technology, ignoring the business side of it completely.

Within domain number one, the organisation itself, certain key role-players are identified. Keep in mind that these role-players may furthermore be subdivided into primary and secondary role-players. The importance of this division is two-fold: (i) different role-players will be allotted different degrees of responsibility for information security; and more importantly (ii) the ultimate responsibility for information security will reside in the primary role-players. Therefor, it is expected of these entities to take full responsibility for any and all information security-related issues.

Primary role-players:

(i) The board and senior management

Ownership for information security resides in the board of directors. The board will ultimately be held responsible if reasonable steps are not taken to protect the information assets of the organisation.[41] Consequently, the board has a "duty of care to ensure that due diligence is paid to information security. To discharge that responsibility they must ensure that responsibility and authority are delegated throughout the organisation."[42]

A critical success factor to any information security initiative is top management support, involvement, and commitment to the process. Top management will therefor have to be involved in: (i) decisions surrounding resource allocations for information security efforts; (ii) aspects surrounding the information security budget;[43] (iii) the development, implementation and

---

41 (n 13) 13.

42 Taylor "Information security principles" (last visited 24 July 2003) http://www.martin.taylor.clara.net/TaylorMaid/SecPrinciples.html 2.

43 (n 13) 13.

integration of the risk management process into the organisation as a whole; [44] and (iv) the monitoring, maintenance and evaluation of the risk management process on a continuous basis. [45]

Secondary role-players:

(ii) Chief Information Officers (CIO)[46]

The Chief Information Officer (henceforth CIO) forms an integral part of the executive team. His function within this team would be to give advice and direction on IT-related issues.[47] Furthermore, he serves as a communication channel between top management, information security professionals and end-users.

The CIO must provide leadership in the development and implementation of all IT initiatives. [48] This would inevitably require of him to focus on at least three broad issues:

(a) Providing IT strategic direction:

- Strategic alignment of IT mission, goals and objectives with the overall mission, goals and objectives of the organisation; [49]
- Participate in long-term strategic planning in order to unleash IT's full potential; [50]
- Build credibility for IT; [51] and

---

44 ibid.
45 ibid.
46 The position of Chief Information Officer is of such great importance that US Congress demands of all executive departments and agencies to create and fill this position. This was done through provisions in the Clinger-Cohen Act of 1996.
47 Tudor *Information Security Architecture* (2001) 28.
48 (n 47) 29.
49 ibid.
50 ibid.
51 ibid.

- Communicates how IT will fulfill organisational objectives. [52]

(b) IT plans and architecture; user interfaces:

- Make IT an integral part of business; [53]
- Provide training to employees, not only to inform and to keep them up to date on the latest technological developments, but also to give them a clear understanding of their role and responsibility for IT; [54] and
- Ensure that when performance measurement is carried out the performance of the IT department of the organisation is not neglected. [55]

(c) Resource allocation:

- Focuses on IT investment decisions, decisions surrounding outsourcing, and budget controls. [56]

Within the information security domain it is expected of the CIO to (i) inform top management and the board of risks associated with the implementation of new technology; and (ii) inform and convince the board and top management of why the need for information security exists. [57]

52 ibid.
53 ibid.
54 ibid.
55 ibid.
56 ibid.
57 ibid.

(iii) Chief Financial Officer (CFO)

The Chief Financial Officer is the principal accounting officer. [58] He is concerned with all activities relating to the financial health of the organisation. His role within the information security domain directly relates to risk management, as a security incident or breach will have a significant detrimental effect/impact on the financial position of the organisation. [59]

(iv) Security Officer

Security officers are wholly responsible for the organisation's information security activities and initiatives.[60] This person will normally be a member of the Executive Committee for Security as well as a member of the Security Team. [61] The responsibilities of the security officer will range from the development, implementation, coordination, and monitoring of: (i) the risk management process; (ii) information security documentation, including information security policies, procedures, standards and guidelines; and (iii) the information security awareness and training program that will inform employees of their roles and responsibilities for information security within the organisation. [62] It should however be kept in mind that it can not be expected of the security officer to perform all of these tasks himself. He is therefor allowed to delegate certain functions to designated employees. It is however expected of him to ensure that these designated employees comply with his directives.

(v) Security Team

The security team acts as advisors and consultants to management on information security-related issues. [63] Their function within the organisation may range from informing management of the latest threats and risks facing

---

58 ibid.
59 (n 47) 30.
60 ibid.
61 ibid.
62 ibid.
63 (n 47) 31.

the organisation, to making recommendations on safeguards and control measures that should be implemented to reduce risks to acceptable levels. [64]

As with the security officer, the security team will be involved in the development and execution of: (i) the risk management process; (ii) information security policies, procedures, standards and guidelines; and (iii) the information security awareness and training program.[65] They are therefor responsible for institutionalising information security within the organisation.

(vi) Security Coordinator

The main function of a security coordinator is to ensure that information is only available to authorised users. [66] It is expected of this person(s) to coordinate his efforts with that of the human resources department to ensure that an ex-employee will not be able to gain access to the organisation's system or network. [67]

(vii) Department Managers

Each department manager will be responsible for the information used within his specific department. Therefor, this person will have to establish an information security strategy for his department. [68] This would entail giving due consideration to: (i) asset classification; (ii) determining who has access to what; (iii) for how long; and (iv) what the user will be allowed to do. [69]

---

64 ibid.
65 (n 47) 32.
66 ibid.
67 ibid.
68 (n 47) 33.
69 ibid.

(viii) Network and Application Administrators

These employees are solely concerned with the technical component of information security. [70] They will for instance implement the security safeguard and control measures decided upon during the risk mitigation process.

(ix) Human Resources Department

Within the information security domain this department has a three-fold function. Firstly, it is expected of human resources department (henceforth HR) to recruit, screen and hire appropriate candidates that will fit into and promote the organisation's culture of security; secondly, to inform the security coordinators immediately upon terminating an employee's employment, in order to ensure that an ex-employee can no longer gain access to the organisation's system or network; and thirdly, it is the responsibility of the HR department to ensure that employees read and understand information security documents. [71] This would inevitably include any future amendments or modifications made to these documents.

(x) Legal Council

It is strongly recommended that legal council form part of both the Executive Committee for Security, as well as of the Security Team. [72] It is expected of the legal council to be involved in: (i) the drafting of information security documentation in order to ensure that it is legally binding on employees; (ii) the enforcement of security documentation which could result in termination of employment; (iii) if the latter does occur it is incumbent on the legal council to gain assurance that the correct procedures are followed in order to avoid disputes in the future based on unfair dismissal and/or unfair

---

70 (n 47) 34.
71 ibid.
72 ibid.

discrimination; (iv) keep management informed of all new legislation and relevant regulations that will impact on the organisation's information security; and (v) address issues pertaining to corporate and personal liability for failed information security, which would include holding those responsible for information security accountable, and prosecute those who violate security. [73]

2.7 Semantics of information security

2.7.1 Components of information security

Information security comprises of three essential components, namely

(1) Physical security;

(2) Technological security; and

(3) Non-technological / procedural security.

All three components must be used in conjunction with one another.[74] If any one of these components is neglected it will result in a vulnerability being exploited not only in that one component, but in the organisation as a whole, as all of these components function interdependently of one-another. It is therefor suggested that a layered approach to information security is followed that embodies all three components. [75] The challenge to organisations will lie in finding the right balance between protecting their information assets, while not inhibiting the organisation's performance. [76]

It should furthermore be borne in mind that all of these components have legal consequences embedded in them. These consequences are however widely unknown and/or ignored. [77]

---

73 (n 47) 34-35.
74 (n 16) 18.
75 ibid.
76 ibid.
77 (n 42) 3.

What follows is a brief overview of what each component entails:

(i) Physical security

Physical security, in stark contrast to its counterparts, is the one security measure that organisations have succeeded in implementing successfully. Its importance is widely acknowledged and understood. [78]

Physical security may be defined as "…methods that protect physical facilities from loss or destruction."[79] Physical security is concerned with: (i) securing the environment within which the information is processed; as well as (ii) physical access to the equipment itself.[80] Keep in mind that physical security is not solely concerned with controlling physical access to a location.[81] It should also provide a mechanism to protect against natural and man-made disasters, such as fires, flooding, humidity and loss of electric power supply. [82]

Physical security is often referred to as the organisation's first line of defense, the reason for this being that "if the system itself is not physically secure, nothing else about the system can be considered secure."[83]

Physical security will be concerned with the following factors:

(a) Location of the facility; [84]

(b) Layout of the facility; [85]

(c) Construction of the facility; [86]

---

78 (n 47) 15.
79 O'Brien *Management Information Systems* (1996) 585.
80 (n 42) 4.
81 Rustad and Daftary *E-Business Legal Handbook* (2002) 173.
82 ibid.
83 Nilsen "Protection of information assets" (last visited 27 February 2003) http://www.sans.org/rr/securitybasics/info_assets.php 2.
84 ibid.
85 ibid.
86 ibid.

(d) Access control to the facility; [87] and

(e) Monitoring access. [88]

Examples of physical security include:

(a) Limiting physical access to the computer room; [89]

(b) Use remote televisions to monitor premises; [90]

(c) Chain link fences;[91]

(d) Automatic alarms;[92]

(e) Keyboard locks;[93]

(f) Alarms;[94]

(g) Smoke detection;[95]

(h) ID tokens;[96] and

(i) Keypads.[97]

(ii) Technological security

"Technology provides the mechanism to enforce policies, standards and procedures."[98]

Technical security may be defined as "…controls implemented through hardware and software that are typically difficult to defeat, and once implemented, can work without human intervention."[99] Technical security would entail the development, acquisition and implementation of technical systems to improve security. This component of information

87 ibid.
88 ibid.
89 Applegate, McFarlan and McKenney *Corporate Information Systems Management* (1999) 240.
90 ibid.
91 ibid.
92 ibid.
93 (n 47) 15.
94 ibid.
95 ibid.
96 ibid.
97 ibid.
98 Tipton and Krause *Information Security Management Handbook* Vol 2 (2001) 233.
99 (n 98) 15.

security evolves around the five pillars of information security, namely identification and authentication; authorisation, confidentiality, integrity, and non-repudiation.[100]

The implementation of technical security measures have as its aim:[101]

(a) **Prevention** – The aim of these measures are to prevent the security incidents from occurring altogether;[102]

(b) **Detection –** Detective measures alert the organisation if a security breach or incident is occurring, or has occurred;[103]

(c) **Mitigation** of risks; [104] and

(d) **Limiting** the **impact** of a breach.[105]

Examples of technological security include:

(a) Encryption;[106]

(b) Public key infrastructure; [107]

(c) Firewalls; [108]

(d) Virtual private networks;[109]

(e) Biometrics;[110]

(f) Remote access servers;[111]

100 (n 42) 3.
101 (n 35) 64.
102 Examples of preventative measures include access controls and authentication tools.
103 Examples of detective measures may include virus-checking software. As pointed out earlier in this chapter organisations should ask themselves two questions concerning detection: (i) when will they be able to detect a security breach/incident? and (ii) will they be able to measure the impact of the security breach/incident?
104 (n 35) 64.
105 ibid.
106 (n 47) 201.
107 (n 47) 208.
108 (n 47) 212.
109 ibid.
110 ibid.
111 ibid.

(g) Digital signatures;[112]

(h) Intrusion detection; [113]

(i) Passwords; [114]

(j) Smart cards; [115] and

(k) Anti-virus software.[116]

The reader should keep in mind that technical details of devising and incorporating technological security measures are beyond the scope of this dissertation.

(iii) Non-technical / procedural security

Procedural security may be defined as dealing with "…persons involved with the use and maintenance of the information and the system."[117] This component is concerned with the administration of technical security through the development and implementation of information security policies, procedures, standards and guidelines.[118]

Policies may be defined as documents:

> "…designed to inform all individuals operating within an organisation of how they should behave related to a specific topic, how the executive management feel about the topic, and what specific actions the organisation is prepared to take related to the topic." [119]

Policies are mandatory.

---

112 (n 47) 15.
113 ibid.
114 It is contended by Schneier *Secrets and Lies* (2000) 136 that the concept of a password is based on an oxymoron. "The idea is to have a random string that is easy to remember. Unfortunately, if it's easy to remember, it's something nonrandom like."
115 (n 47) 15.
116 ibid.
117 (n 42) 3.
118 ibid.
119 (n 47) 79.

Standards are defined as being "…specific set of rules, procedures or conventions that are agreed upon between parties in order to operate more uniformly and effectively."[120] These are mandatory.

Procedures may be viewed as "giving guidance and typically answers the more detailed question of where, when, and how, while policy answers who, what and why."[121] These are mandatory.

Guidelines are "general statements that are designed to achieve the objective of the policy by providing a framework within which to implement procedures."[122] These are optional.

120 ibid.
121 (n 47) 80.
122 Tipton and Krause *Information Security Management Handbook* Vol 3 (2002) 374.

The chain of command that exists amongst these security documents is depicted below:

Corporate Policy

("States goal in general terms.")[123]

Standard

("Define what is to be accomplished in specific terms.")[124]

Procedure

("Step-by-step reference guide telling employees how to meet the standards.") [125]

Guidelines

("These are general recommendations of what organisations would like to see its employees do.")[126]

123 Peltier *Information Security Policies, Procedures, and Standards* (2002) 70.
124 ibid.
125 (n 122) 365.
126 (n 122) 365-366.

2.7.2 Building blocks of information security

A fundamental tenet of information security is to protect its **five pillars/building blocks** namely:

(i) Identification and authentication;[127]

(ii) Authorisation;[128]

(iii) Confidentiality;[129]

(iv) Integrity;[130]and

(v) Non-repudiation.[131]

(vi) The researcher identifies an additional pillar, namely availability.[132]

These five pillars, their corresponding objectives, and the technological solution assigned to them, are depicted below:[133]

[127] Unknown "PKI addresses six pillars of information security" (last visited 18 February 2002) http://www.computingsa.co.za/2001/05/21/Communications/sec01.htm 2.

[128] ibid.

[129] ibid.

[130] ibid.

[131] ibid.

[132] ibid.

[133] These five pillars are generally referred to as services. It is contended by Von Solms, Eloff HP, Eloff M. and Smith *Information Security* (2001) 2 that by managing and implementing these services a comprehensive understanding of information security may be gained. Keep in mind that information security literature generally only refers to five pillars/building blocks of information security, namely identification and authentication; authorisation; confidentiality; integrity and non-repudiation. Availability is therefor omitted. The researcher did however include this as a sixth pillar, because of its importance.

Security Issue	Security Objective	Security Technique
1. Identification and Authentication	Origin verification	Digital signatures Challenge-response Passwords Biometric devices
2. Authorisation (Logic Access Control)	Limiting entry to authorized users	Firewalls Passwords Biometric devices
3. Confidentiality	Privacy of message	Encryption Cryptography
4. Integrity	Detecting message tampering	Hashing Digital signature Encryption Message authentication codes (MACs) and message digests
5. Non-repudiation / Non-denial	Proof of origin, receipt and contents (sender cannot falsely deny sending or receiving the message)	Bidirectional hashing Public key encryption Digital signatures Transaction certificates Time stamp Confirmation services
6. Availability	Verification Ensures availability to authorised users	Disaster recovery Business continuity

Discussion of the diagram:

Security Issue	Security Objective	Security Technique
1. Identification[134] and Authentication[135]	Origin verification	Digital signatures[136] Challenge-response[137] Passwords[138] Biometric devices[139]

[134] Authentication and identification are two notions that are very tightly bound, yet they are not synonymous with one-another. Identification of the user is the first step that will take place. Only once the identity of the user has been verified can the next step authentication take place. Panis and Hellstrom "The IDA programme – legal and security aspects" 4 (1997) *The EDI Law Review* 176 define identification as: "…the process of ascertaining the identity of a participant by relying on unique distinguishing features."

[135] Tipton and Krause (n 98) 233 define authentication as: "…the process by which access is established and the system verifies that the end user requesting access to the information is who they claim to be." Therefor authentication is concerned with the identification of the sender of the document with absolute certainty. It encompasses anonymity. Authenticity is defined by Panis and Hellstrom "The IDA programme – legal and security aspects" 4 (1997) *The EDI Law Review* 176 through the fulfillment of three features:

(i) Proving that the person who claims to have signed the document actually did so (Paternity);
(ii) Proving that the document was not altered since signature (Integrity); and
(iii) Preventing a digital signer from later asserting that he did not sign (non-repudiation)."

The service of identification and authentication has a two-fold purpose: (i) to prevent intruders from impersonating legitimate users of an IT system; and (ii) give the assurance that only legitimate users of a system have access to the system." It should furthermore be observed that the enforcement of identification and authentication is easier in a closed environment than in an open environment. The reason for this being that in a closed environment pre-registration of the user is require, this is however not required in an open environment. Von Solms, Eloff HP, Eloff M. and Smith *Information Security* (2001) 22. The ECT ACT 25 of 2002, chapter six makes specific reference to authentication, and more specifically to authentication service providers. Section 37 provides that the Accreditation Authority may accredit authentication products and services that support advanced electronic signatures, subject to the fulfillment of certain conditions.

[136] The important role digital signatures play in the information age is evident from legislation, such as the ECT Act 25 of 2002, that deals comprehensively with this subject-matter. Section 1 of the ECT 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." By drawing a distinguishing between an advanced electronic signature, and a 'normal' electronic signature, it would appear as if the Act implies that the former will carry more evidential weight than the latter. Furthermore, section 13 of this Act deals specifically with signatures and the legal consequences attached to them. It is clear that "(t)he Act aims to give the same legal effect to digital signatures, which includes both advanced electronic signatures and ordinary electronic signatures, which traditional signatures enjoy in our law" Jansen "A new era for e-commerce in South Africa" (October 2002) *De Rebus* 17. Keep in mind that a digital signature uses public key infrastructure (PKI) to: (i) authenticate the sender; and (ii) verify the content of the document.

[137] Greenstein and Vasarhelyi *Electronic Commerce* (2002) 336 define the challenge-response technique as: "…an interactive procedure in which on the one end (the user) must prove something by answering a challenge to the other end (the host computer or authenticator)."

[138] Rustad and Daftary (n 81) 1176 defines a password as: "…a secret sequence of letters and other symbols needed to log on to a computer system as an authorized user."

[139] Biometric devices require "…that some physically unique characteristic of the user be used for identification..." Greenstein and Vasarhelyi *Electronic Commerce* (2002) 336.

Security Issue	Security Objective	Security Technique
2. Authorisation[140] (Logic Access Control)	Limiting entry to authorized users	Firewalls[141] Passwords Biometric devices

[140] In its most simplistic form authorisation describes who has access to what.

[141] SANS "NSA glossary of terms used in security and intrusion detection" (last visited 27 February 2003) http://www.sans.org 6 defines a firewall as: "(a) system or combination of systems that enforces a boundary between two or more networks. Gateway that limits access between networks in accordance with local security policy."

Security Issue	Security Objective	Security Technique
3. Confidentiality[142]	Privacy of message	Encryption[143] Cryptography[144]

[142] Confidentiality ensures that information may only be observed, used or disclosed to those people with necessary authorisation, and encompasses security and privacy concerns. Confidentiality is therefor concerned with protecting the content of information against unauthorised disclosure or interception. This is true regardless of "where the information resides or how it is stored" Ernst & Young (n 36) 8; Tudor (n 47) 1. Various information security models exist that are based on the five pillars of information security. There are however three principal security models, the first of which being the Bell and Lapadule model. This model is one of the best known and most widely used information security models. It is a confidentiality-based model for information security, that is based on two rules relating to (i) the reading of the data; and (ii) the writing of the data. In essence this model provides that "(a) subject can read from objects with a security class on the same or lower level. A subject can write to objects on the same or higher level" Tipton and Krause (n 122) 354.

[143] Greenstein and Vasarhelyi *Electronic Commerce* (2002) 312 define encryption as: "…the transformation of data, via a cryptographic mathematical process, into a form that is unreadable by anyone who does not possess the appropriate secret key." Basically two forms of encryption exist, namely symmetric encryption/secret key encryption and asymmetric encryption/public key encryption. The former "…uses a mathematical formula (algorithm) for encrypting (scrambling) the data, and the decryption process uses the same mathematical formula (algorithm) for decrypting (unscrambling) the data…"; whereas in the latter case "…different but related algorithms and different but related keys are used for encryption and decryption" Von Solms, Eloff HP, Eloff M. and Smith *Information Security* (2001) 16.

[144] Cryptography represents a more general concept, which includes not only encryption, but also decryption, authentication, digital signatures, paternity, integrity, non-repudiation, key management and key certification. It is a coding method in which data is encrypted and then decrypted using algorithm. Greenstein and Vasarhelyi *Electronic Commerce* (2002) 336. The ECT Act 25 of 2002 makes specific reference to cryptography. Section 1 of the Act 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."

Furthermore, chapter five of the Act deals specifically with cryptography providers.

Security Issue	Security Objective	Security Technique
4. Integrity[145]	Detecting message tampering	Hashing Digital signature Encryption Message authentication codes (MACs) and message digests[146]

Security Issue	Security Objective	Security Technique
5. Non-repudiation /Non-denial	Proof of origin, receipt and contents (sender cannot falsely deny sending or receiving the message)	Bidirectional hashing Public key encryption Digital signatures Transaction certificates Time stamp[147] Confirmation services

[145] Information must be protected against unauthorised, accidental or intentional modification or alteration. The goal of integrity is to offer users accurate, complete information that is current. IT Governance Institute (n 13) 9. The remaining two information security models, namely the Biba model, and the Clark-Wilson model are both integrity-based models. The purpose of the Biba model is to fulfill the first and foremost objective of integrity, namely to prevent unauthorised users from making modifications to information. This model is furthermore based on "a hierarchical lattice of integrity levels, the elements of which are a set of subjects (active information processing) and a set of passive information repository objects." The Clark-Wilson model addresses three goals of integrity, namely:

(i) Preventing unauthorised users from making modifications;
(ii) Maintain internal and external consistency; and
(iii) Preventing unauthorised users from making improper modifications.

This model is based on well-informed transaction. It is interesting to observe that integrity models are generally in conflict with confidentiality models. Tipton and Krause (n 122) 355.

[146] Keep in mind that when using MACs and message digest only the integrity of the message will be protected, and not its confidentiality. Von Solms, Eloff HP, Eloff M. and Smith *Information Security* (2001) 18.

[147] Digital time stamping is used to "… determine the exact time in which a message was created, while a message service can attest to the exact time the message was sent and received " Greenstein and Vasarhelyi *Electronic Commerce* (2002) 336.

Security Issue	Security Objective	Security Technique
6. Availability[148]	Verification.[149] Ensures availability to authorised users	Disaster recovery Business continuity

All six pillars are first and foremost concerned with access control.[150]

[148] The reader should be mindful of the fact that information security literature generally only refers to five pillars/building blocks of information security, namely identification and authentication; authorisation; confidentiality; integrity and non-repudiation. Availability is therefor omitted. The researcher did however include this as a sixth pillar, because of its importance. Availability is concerned with ensuring that information is available to authorised users when required. The two notions of availability and reliability should however not be confused. The distinction is important because ensuring availability will not be delivered by implementing reliability. Reliability is concerned with trustworthiness. Therefor, something that may be relied upon Warman (n 14) 93. It is suggested by Tudor (n 47) 2 that there are two issues affiliated with availability, namely (i) denial of service caused by lack of security controls; and (ii) loss of services from information resources due to natural disasters.

[149] Verification ensures information is being used for the purposes authorised and intended.

[150] The practical application of these five pillars in a closed environment would be as follow:

(i) IT system will identify the potential user by checking if the user-id offered to the system appears in its database;

(ii) IT system verifies that the user-id really belongs to the person offering the user-id;
This will be done by making use of, or combining three methods:
- Something the user knows (eg. password);
- Something the user possesses (eg. magnetic card; memory card; smart card);
- Something the user is (biometrics eg. fingerprint; palm print; voiceprint); or
- A combination of all three methods.

(iii) IT system must now allow signed-on user selective access to those resources to which he/she is authorised;

(iv) IT system must furthermore ensure that only authorised persons view the contents of the data;

(v) IT system must allow only authorised users to modify protected objects, such as messages, databases and programs; and

(vi) There must be some form of proof that the transaction did in fact take place, and an identification of the parties between whom the transaction took place. This will ensures that a person can be held accountable for his actions at a later stage.

Keep in mind that each step will act as a continuation of the previous step and is dependent on the fulfillment of the requirements of its predecessor. Von Solms, Eloff HP, Eloff M. and Smith *Information Security* (2001) 1–132.

2.8 Regulating information security[151]

Information security is regulated by means of:

(i) Legislation;

(ii) Regulations; and

(iii) Standards.

(i) Information security legislation

Two questions must be addressed under this heading:

(i) What are the laws governing information security? and

(ii) Do such laws even exist?

Before answering these two questions the reader must be mindful of the fact that the law and technology are two very distinct disciplines.[152] It would appear as if the law always lags far behind technology. Holmes[153] correctly observed that "it cannot be helped, it is as it should be, that the law is behind the times."

This problem arose as a direct result of the convergence of the following factors:

(i) The rapid rate at which new technology is developing, and old technology becomes absolute, makes it impossible for the law to keep up with changes occurring in this field;[154]

---

[151] For a comprehensive list of national and international information security legislation, regulations and standards, consult Annexure A.

[152] Various problems are experienced when the two disciplines law and information security meet, specifically when considering liability for failed information security. Lawyers who are expected to defend or prosecute cases dealing with failed information security generally lack the necessary insight into this discipline. This problem is exacerbated by the fact that lawyers generally lack a basic understanding of computers and related technologies. Consequently, the question that begs to be answered is: "do we make security experts lawyers, or do we make the lawyer security experts?" Philip "The legal system and ethics in information security" (last visited 27 February 2003) http://www.sans.org/rr/legal/system.php 2.

[153] *Speeches* (1934) 102.

[154] Philip "The legal system and ethics in information security" (last visited 27 February 2003) http://www.sans.org/rr/legal/systems.php 2.

(ii) Law is reactive in nature. The law does not predict crimes to be committed in the future, but reacts to crimes committed in the past; and

(iii) The drafting and enactment of new legislation is a cumbersome and time-consuming exercise, which can take months or even years to complete.[155]

Returning to the two initial questions, it may be observed that in South Africa, at present, there are no laws regulating information security **per se**. However, there is an ever-increasing volume of legislation **impacting** on information security. These pieces of legislation will cover a wide realm of law, ranging from data protection, data privacy, software copyright, certification standards and guidelines.

In the absence of information security legislation, organisations will have to look to information security regulations and standards for guidance.

(ii) Regulations and Standards

A clear distinction should be drawn between regulations and legislation. Regulations are sector specific.[156] Therefor, organisations will only have to comply with the regulations applicable to the specific sector in which it function or operate. In contrast to this, legislation will be applicable to organisations irrespective of the sector in which they function and operate. [157] Legislation therefor extends across all sectors.

---

[155] In South Africa the following process will take place before a law will come into force:
(i) Experts draft a Bill;
(ii) The Bill is published in the Government Gazette to allow for public comment on the Bill;
(iii) The Minister presents the Bill before parliament;
(iv) Parliament committees report back to parliament;
(v) Parliament votes on whether or not to pass the Bill;
(vi) If the Bill is passed, the president signs it; and
(vii) The statute is published in the Government Gazette.

[156] Lycett "Information security: regulation and legislation" (last visited 29 May 2003) http://www.infosecnews.com/opinion/2003/03/12_04.htm 1.

[157] ibid.

The question may be asked what is the position of regulatory bodies concerning information security?

As mentioned earlier regulations are sector specific. Therefor the type of regulation that will be applicable to an organisation will depend on the nature of the organisation and the sector in which it operates.[158] There is however one regulation that extends across all sectors, namely corporate governance.[159] Corporate governance is concerned with "the way in which companies are managed."[160] In South Africa corporate governance is embodied in the King II Report on Corporate Governance 2002. Therefor, all organisations, irrespective on the nature of their business will have to give regard to the provisions of the King II report.

(iii) Standards

Organisations may look to information security standards for guidance when wanting to implement or benchmark their information security efforts. Organisations will do well to focus on at least one of the following information security standards:

(a) ISO 17799;[161]

(b) COBIT;[162] or

---

158 Examples of these sectors would include the banking sector or health care sector. Lycett (n 156) 1.

159 The notion of governance and specifically corporate governance from a South African perspective is discussed in greater detail in chapter three hereafter.

160 (n 156) 1.

161 ISO 17799 was developed by the International Organisation of Standards. The aim of this document is to provide organisations with a single reference point for information security management. ISO 17799 is discussed in greater detail in chapter six hereafter. Also see Annexure A.

162 Control Objectives for Information and Related Technology (COBIT), was developed by the IT Governance Institute. COBIT may be defined as: "…an open-standard IT control framework that starts from the premise that IT needs to deliver the information that the enterprise needs to achieve its objectives" Appleby (ed) "Closing the governance gap: bringing boards into the IT equation" (August 2001) Vol 7 Number 7 *Information Edge* 5. For a more comprehensive discussion on this standard, consult Annexure A.

(c) OECD Guidelines for Information Security Systems and Networks.[163]

It should however be kept in mind that global enforcement of information security is, at this stage, a security fantasy. [164] Furthermore, it must be realised that at present it can not be expected of South Africa to become a leader in the field of information security. The best South Africa can hope to achieve is to obtain the "first-adopter" advantage.

2.9 Conclusion

In the pursuit of information security the following sentiments about this discipline must be kept in mind. Firstly, information security is a business problem, not a technology one. Consequently, 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.

Secondly, information security is a process, not a product. As a process it has various components (physical, technological and non-technological/procedural) that should be considered. The better these components fit together, the more efficiently and effectively information security will be used within the organisation.

Lastly, information security is a chain; it is only as secure as its weakest link, and within any organisation the weakest link will inevitably be humans, therefor the organisation's own employees.

---

[163] Organisation for Economic Co-operation and Development (OECD) developed guidelines for information security systems and networks. For a more comprehensive discussion on this standard, consult Annexure A.

[164] (n 15) 4.

Information, as an asset of the organisation, can no longer be defined and kept within the corporate walls. [165] Yet, despite the value information holds to the organisation, information security is sill viewed as an afterthought. Consequently, most organisations will only focus their attention on information security once a security incident or breach has occurred. They take a reactive approach to it. It should however be kept in mind that "prevention is better than cure. It is cheaper in the long-run, and far less painful."[166]

This chapter presented a brief overview of some of the basic concepts and principles underlying information security, thereby enabling directors and top management to gain a basic understanding of what this discipline entails. Attention must now be focused on the question why information security needs to be governed in the first place.

[165] 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 3.

[166] KPMG "Information security survey 2000" (last visited 28 June 2001) 3.