TABLE OF CONTENTS

LIST OF APPENDICES

LIST OF FIGURES

LIST OF TABLES

CHAPTER ONE

NATURE AND SCOPE OF THE STUDY

1.1 INTRODUCTION

Most organisations around the world, and also in South Africa, have developed websites for information and business related purposes (Singh, 2010; Siponen, Mahmood & Phahnila, 2014). Some of these websites merely display information about the organisation, whilst others offer some interactivity with customers. The Internet revolution is expanding rapidly due to electronic commerce (e-commerce) (Chambers-Jones, 2013). It is on this premise that most organisations are striving to catch up. De Kare-Silver (2001) noted more than a decade ago, that it was a daunting task for organisations to master the new environment, explaining that: "There is a new game in town and it is now about learning and embracing the new factors for success." These words are now even more applicable in e-commerce (Abawajy, 2014).

According to Ginn (2013) and Siponen et al. (2014), the challenges brought by the Internet to the corporate environment are exacerbated by information security risks, threats and crime.

Hanser (2011) and Ginn (2013) observes that although information security is essential to be able to use the information resources, it is not just information security that organisations need to achieve. Users should be able to trust the infrastructure on which they rely to facilitate their private and business transactions (Mukundan & Sai, 2014). Be that as it may, trust in e-commerce is a product of dependable information security. Chambers-Jones (2013) claims that information security is e-commerce's Achilles heel. Maskerville, Spagnoletti & Kim, 2014) reports that the business-to-consumer component of e-commerce may be affected by reservations regarding information security breaches. On the other hand, the credit card is the most common online payment option and thus both e-commerce customers and merchants are vulnerable to potentially high levels of fraud due to stolen cards and illegally acquired card numbers (Rahman & Ramos 2013; Maskerville et al. 2014). Although new technical techniques are constantly being developed to deal with online fraud, these techniques are not necessarily fool proof and a perfect method of encrypting has not yet been developed. It is on the basis of this premise that information security measures cannot be left to technical techniques only (Panton, Colombi, Grimaila & Mills, 2014).

Similarly, dealing with electronic crime also cannot be left only to organisations in the corporate environment. According to Campbell (2005), several governments have developed legal requirements regarding e-commerce. The challenge is how to regulate the e-commerce activities through national regulation since the Internet transcends geographical boundaries (Junio, 2013; Maskerville et al., 2014). Westby (2013) argues that some governments are stricter than others, but they do not have the right to impose their laws and standards on other countries.

South African e-commerce merchants and consumers are not immune to cyber-crime (Masete, 2012; Panton et al., 2014). The South African government promulgated the Electronic Communications and Transactions Act No. 25 of 2002. Both the King II (2002) and King III (2009) reports contained good governance recommendations which deal with information security issues. Prior to the Electronic Communications and Transactions Act No. 25 of 2002 and the King II Report of 2002, South African e-commerce merchants and customers relied on common law (Dunlop, 2005). The legislation that was introduced through the ECT Act has given e-commerce participants confidence in transacting over the Internet (Luyinda, Herselman & Botha, 2008; Haar, Norlyk & Hall, 2014).

The contribution of legislation and organisational policies in providing information security in e-commerce transactions needed to be investigated in the South African corporate environment. To date, little research has been conducted in this area. For the purpose of this study, the terms ‘organisation’ and ‘company’ were regarded as having the same meaning and were therefore used interchangeably.

1.2 BACKGROUND

This section will provide an overview of the issues that are related to e-commerce, information security threats, risks and crime, and legal and policy aspects of information security. The section will also examine the legal framework of cyberlaw in the South African context.

1.2.1 E-commerce and information security

The terms ‘e-commerce’ and ‘information/knowledge economy’ are synonymously used by a number of authors (Hanser, 2011). Agwu (2013) reports that e-commerce is based on the increased salience of information as a commercial resource. The use of information resources is rapidly becoming central to the competitiveness of organisations. This assertion is supported by Bellovin (2013), who argues that the competitiveness brought about by e-commerce reflects the significance of Information and Communications Technologies (ICT) as enabling tools in online transactions. This is largely attributed to the growth of the Internet.

ICT was the catalyst for the electronic transformation which has shifted from wealth based on goods manufacturing to that based on information resources (Luyinda et al., 2008;Trope & Humes, 2013). According to Wu (2013), the increased use of information by organisations for commercial purposes leads to new industrial structures, services and products. The most discernible indication of transformation is the transition from a marketplace to the Internet where business transactions take place in a wider area without physical contact (Sood & Enbody, 2013). It is noted that the world in which the information economy functions is characterised by globalisation and disintermediation, yet life in the digital world relies on support from bricks-and-mortar life. The drivers of globalisation are intricately bound to the world of the information economy (Siponen, Mahmood & Pahnila, 2014). Both electronic merchants and consumers need to be aware that e-commerce exists in the real world. It is essential to bear in mind that amidst the excitement of ICT, there are people involved. As in the real world, some of the people involved in e-commerce are vulnerable to risks, threats and crimes (Lu, 2013; Corrado, 2013). It is on the basis of this premise that there is a business case for information security.

Whilst several organisations are developing and implementing information security measures, national governments in countries in which they are based are introducing legislative measures in order to deal with information security issues (Campbell, 2005; Corrado, 2013), and the current research explains how countries such as the Czech Republic, Hungary, India and Malaysia have employed national laws to deal with information security risks, threats and crimes. Although national governments are responsible for introducing legislation and policy direction regarding information security, organisations should also develop policies at a micro level (Nikolayevich & Borisovna, 2014). It was stated in the introductory section of this study that information security measures should not be confined to technical protection measures only. It is the view of the researcher that technical measures should be employed within a particular legal and policy framework. This study attempts to assess the impact of the information security legal and policy aspects on e-commerce in the South African context.

1.2.2 Information security risks, threats and crime

While information resources are essential in participating in e-commerce and/or the information economy, they are not exempt from risks, threats and crime (Nikolayevich & Borisovna, 2014). It is therefore advisable for any organisation that uses information resources to have the necessary information security in place. Information security provides e-commerce merchants and consumers with a false sense of safety and freedom from risks, threats and crime. It has been observed that in e-commerce four different places are involved: the location of the user, the location of the Web server, the location of the Web owner, and the virtual location of the site, and thus information security is a central concern (Tiwari, 2013).

Privacy is one of the challenges regarding information security. This, according to Charlesworth and Pearson (2013), is a major challenge for any financial transaction in the e-commerce environment. As far as privacy in e-commerce is concerned, the literature reflects three main areas of concern:

- *personal privacy*, so that unauthorised entities and individuals should not obtain illegal access to private and personal information (McLaughlin & Devers, 2012);
- *confidentiality*, therefore information should be protected from unauthorised individuals and organisations (Charlesworth & Pearson, 2013), and
- *obstruction and destruction* by third parties or hackers (Pellot, 2013).

The processing of e-commerce transactions raises the issue of information security. Mahadeo and Shivaji (2013) report that during the early era of e-commerce, the Internet was generally regarded as being an unprotected medium. This perception, rightfully so, continues to persist (Nye, 2013). News of hackers and online fraudsters made headlines and led to fear amongst millions of potential electronic shoppers (Rogerson & Milton, 2013), who believed that the Internet was not a secure environment in which to provide confidential information. This, according to Overill (2013), held the information economy back from even earlier advancement.

It should also be noted that viruses and other forms of hostile code (malware) are universally experienced as an information security problem (Lawande, 2012). The infection rate continues to grow and this also affects e-commerce participants negatively. Malware has the ability to penetrate firewalls, hijack Virtual Private Networks (VPNs) and also defeat digital signatures (Pisaric, 2013). Aggressive code is the most well-known source of information security lapse (Lawande, 2012). Huey, Nhan and Broll (2013) list several examples of malware, including worms, Trojan horses and macro viruses.

Cyber-crime is an extension of traditional crime, but it takes place on the Internet. In this environment, cyber-crime takes on the non-physical nature of cyber-space and becomes borderless, timeless and relatively anonymous (Gabrys, 2004). Cyber-criminals therefore have the potential to reach any networked information resource in the world (Crume, 2000; Aleshnikov & Demin, 2013). In fact, location is becoming irrelevant, due to the spread of wireless and satellite technology. This statement is supported by Dolcil and Macadall (2014), who assert that the global reach of networked information resources is promoting a borderless platform for cyber-crimes. Furthermore, the continuous around-the-clock accessibility to computer systems has made it difficult to trace the tracks of cyber-criminals. Gabrys (2004) has learnt that cyber-criminals take advantage of the Internet by networking with other cyber-criminals and creating gangs.

Although information security risks, threats and crimes are serious problems in the e-commerce environment, it is interesting to note that an organisation like Amazon.com is succeeding in online trading (Kalra & Sood, 2013). It is believed that customers are conducting these kinds of e-commerce transactions because they know that information security can be achieved (*ibid*). It is on this basis that customers should feel secure when they do online shopping (Skoudis, 2004). Kamel and Lanet (2013) have noted that nowadays supplying one’s credit card online can arguably be more secure than providing it over a cell phone or physically handing it over to the seller.

Kalra and Sood (2013) state that organisations that succeed online, are those which post information security policies on their Websites. The policies enable these organisations to explain their commitment to information security and give the customer an extra level of confidence (Mbaku & Yu, 2013; Aleshnikov & Demin, 2013). In most instances, these policies deal with issues related to the credit card numbers and the confidentiality of personal data. Some of these organisational policies are aligned with the laws of the countries in which they operate (Dolcil & Macadall, 2014).

The researcher has noted that organisations in other countries are employing legal and policy aspects in their endeavours to provide information security in e-commerce transactions (Ardito & Procacciant, 2013), and this informs the study which aims to investigate how South African organisations employ legal and policy aspects when they provide information security.

1.2.3 Policy aspects to consider when providing information security

As mentioned, some organisations post their information security policies on their websites to diligently explain their commitment to information security. These policies deal with issues such as the usage of credit cards and other personal data. Bedard (2014) provide an example of how America Online posts a privacy policy on its website regarding the kind of information it collects about people who visit its website. America Online also explains what it does or does not do with the collected personal data.

Information security policy is formulated to inform all individuals who operate within an organisation as to how they should conduct themselves with regard to ICT information security issues (Julisch, 2013). In some instances, policies are formulated because of regulatory requirements (Sharifi & Tripunitara, 2013). Developing information security policies for the sake of satisfying regulatory obligations is not sufficient. The Information security policy is also used as a communication tool amongst the information system stakeholders.

The advancement of the information economy in terms of the rapid growth of e-commerce places an obligation on government and organisations to develop information security policies and regulatory solutions (Corrado, 2013). In the era of information economy, information security policies will assist in providing users with security and privacy assurance (Hassan & Sabry, 2013). However, the differences in policy approaches amongst key role-players and countries make it difficult to provide an adequate information security policy and regulatory framework (Nanevski, Banerjee & Garg, 2013). Although this difficulty emanates from the macro level, it manifests itself at the micro (organisational) level.

The unavailability of information security policies is the most serious security breach for any organisation that has to protect its customers, networks, systems and data (Ruggiano & Brown, 2013). Every organisation should subscribe to policies regarding its business (the business policy), how and with which resources it will achieve its objectives (technical policy), and how it will protect its assets and survival (information security policy) (Zinszer & Tamblyn, 2013). All policies should be documented officially and agreed to by all the stakeholders.

According to Shu'aibu and Sukri (2013), information security policies should be visible in order to be effective. Visibility helps to fast-track the implementation of the policy because the policy is then known throughout the organisation. It is therefore advisable to employ presentations, videos, workshops, speakers, discussion panel fora and newsletters, to name but a few deployment methods (Assaf, 2012; Ruggiono et al., 2013). The organisations' information security training and awareness initiatives can assist in informing users of new information security policies (Demirhan & Demirtas, 2011; Shu'aibu and Sukri, 2013). Information security policies should be introduced in a way that ensures the support of stakeholders, especially in organisations where workers feel overwhelmed by directives and procedures. The information security policy in an organisation can also be seen as a reflection of management's commitment to information security and expectations regarding staff responsibilities, actions and accountability. Information security should also be integrated into other organisational policies. This can be achieved by co-ordinating policies and involving other business units. This will make it easy for users to implement information security policies. Campbell (2005) clearly indicates the role of law in information security.

The following section provides an overview of legal aspects to consider when providing information security.

1.2.4 Legal aspects to consider when providing information security

Countries such the Czech Republic (Loebl, 2005), Hungary (Szeman, 2005), India (Joshi, Salaria & Naidu, 2005), Malaysia (Fatt & Wahjanto, 2005), Singapore (Chia, 2005), Taiwan (Kuo & Fan, 2005), the United Kingdom (Griffiths & Harrison, 2005), and the United States of America (USA) (Weiser, 2005) have developed laws that deal with e-commerce and information security in particular. The governments of these countries have also developed strategies that stimulate the advancement of information security (Salzberg & Jang, 2012). However, according to Sanchez-Pena & Fernandez-Vice (2013), there are countries in which e-commerce and information security are not supported by any legal framework.

Some of the laws passed in various countries regarding e-commerce and information security include the Law of Electronic Communication of 2005 in the Czech Republic (Szeman, 2005); the e-Commerce Act of 2001 in Hungary (Szeman, 2005); the Information Technology Act of 2000 in India (Joshi, Salaria & Naidu, 2005); the Electronic Transactions Act of 1996 in Singapore (Chia, 2005); the Malaysia Digital Signature Act of 1997 in Malaysia (Fatt & Wahjanto, 2005); and the Uniform Electronic Act of 1999 in the United States.

Most governments do not develop a legal framework to stifle e-commerce but rather to create the right conditions in which the information economy can flourish (Loblich & Wendelin, 2012; Salzberg & Jang, 2012). Government intervention in regulation should be in the background rather than at the forefront of the information economy. According to Ardito and Procaccianti (2013), governments' laws and regulations do not always provide the corporate environment with space to formulate and implement its own policies. This may have a negative impact on the growth of emerging technologies. For example, Germany's law on digital signatures imposed inflexible licensing terms on certification authorities (Hamadouche & Lanet, 2013; Sanchez-Pena & Fernandez-Vicente, 2013).

Cecere and Rochelandet (2013) report that pushing through laws regarding eCommerce and information security by governments in several countries has led to the lack of a uniform international legal framework. The nature, scope and transitional nature of the information economy all exacerbate the problem. While Abawajy (2014) supports a common global legal and regulatory framework, Ruggiano and Brown (2013) suggest that the industry should establish its own policies within the national, regional and international legal framework. Although some developed countries have recognised threats posed by inadequate information security, little has been done practically to implement legal measures that will deal with the problem (Ting & Yi, 2013). This can be attributed to differences over the form of such a legal framework. The disputes between the European Union (EU) and the USA over the assorted aspects of the Internet regulatory framework do not help to address the problem. However, there are some attempts being made at the international level to develop a legislative framework for information security (Ardito & Procaccianti, 2013; Borgmann, 2013).

Such attempts include the establishment of the Electronic Signatures Electronic Commerce Directive, as a consequence of various EU initiatives (Borgmann, 2013; Loblich & Wendelin, 2012). The United Nations International Trade Law Commission (UNCITRAL) introduced the Model Law on Electronic Commerce (the 1996 Model Law) in 1996 (Joshi, Salaria & Naidu, 2005). The introduction of the 1996 Model Law emerged from the challenge of developing a regulatory framework for the use of the Internet where existing legal systems were not entirely applicable to electronic transactions. This study investigates how national and international legal frameworks are taken into account by South African organisations when they secure their information resources.

1.2.5 Legal framework of e-commerce and information security in South Africa

There has been a rapid rise in the use of e-commerce in South Africa and the need emerged to develop legislation that would provide security to Internet consumers and merchants (Dunlop, 2005; Pellot, 2013). South African Common Law does not address issues related to the security of electronic transactions sufficiently.

According to Dunlop (2005), the South African government did not confine its concerns to information security, but intended to provide a legal framework that would address security, transparency and infrastructural commercial development. The assumption was that e-commerce initiatives that are based on a sound legal framework would enable South Africa to become a leading technology power on the African continent (Dunlop, 2005; Dagada, Eloff & Venter, 2009). It is on this basis that the South African Department of Communications established an ICT investment cluster in May 1998 to create a legislative framework on issues relating to e-commerce and information security (Groenewald, 2000; Dagada, 2013).

Dunlop (2005) reports that the South African government established a task team in the early 2000s to produce a document that would form a basis for the development of an e-commerce policy, followed by legislation. The legislation was preceded by both a Green and a White Paper (Groenewald, 2000; De Wet & Du Plessis, 2004).

According to Dunlop (2005:560), the South African government prescribed the following objectives in developing an e-commerce policy:

- to create an enabling legal and regulatory environment for open and fair participation in e-commerce;
- to support technological developments that will lead to the establishment of global connectivity;
- to ensure that legal systems and international trade agreements between nations are adjusted and reformed to accommodate the new concepts of law;
- to establish appropriate law enforcement to prevent crimes in the information space; and
- to promote education that will increase information literacy among all citizens.

The following statutory instruments predominantly regulate the South African legal framework regarding e-commerce and information security in particular: Constitution of the Republic of South Africa No. 108 of 1996 (specifically the right to privacy); the Electronic Communications and Transactions Act No. 25 of 2005 (providing the framework behind electronic communications and also addressing cyber-crime – chapter 13, sections 85-89); the Promotion of Access to Information Act No. 2 of 2000 (which deals with records management, disclosure, confidentiality and access); the Regulation of Interception of Communications and Provision of Communication-related Act No. 70 of 2002 (which prohibits interception and monitoring without permission from a Court of Law); the King

Reports on Governance for South Africa (King II, 2002 and King III, 2009); and the Protection of Personal Information Bill No. 9 of 2009 (which deals with the right to privacy). Furthermore, on 27 November 2013, the Protection of Personal Information Act No. 4 of 2013 was signed into law; however, it was not significantly drawn on for the purposes of this research.

The widely used King Reports on Governance for South Africa were named after Advocate Mervyn E. King, SC, Chairman of the King Committee on Corporate Governance (King & Lessidrenska, 2009). This Committee was established in 1992 and issued the first report in 1994 (King, 2006). The King II Report was released in 2002 with a particular emphasis on good governance. It recognised that ICT has the capacity to bring security risks and challenges to the company and the Board of Directors should address this (King II Report, 2002). Inasmuch as the King II Report was not legislation, but rather a set of guidelines, companies listed on the Johannesburg Securities Exchange were compelled to comply with the report. The King II Report was replaced by the King III Report of 2009. One of the major differences between the two reports is that the King III Report has more information security and IT governance provisions than the King II Report, where the King III Report argues that information security is a critical component of the overall efficiency and sustainability of the enterprise.

1.3 THE PROBLEM STATEMENT

As explained in Section 1.2, legal and policy aspects are important in the provision of information security. Although several authors have written about legal and policy aspects regarding information security in the South African context, it has not been explained how these aspects are used in the provision of information security in the South African corporate environment. The question arises as to whether the range of legislation previously mentioned, as well as other information security-related legislation at macro level, and the organisations' policies, are used by South African organisations in their endeavour to provide information security.

According to Reinhardt Buys (2004) of Buys Incorporated Attorneys, "Both the 2002 and 2004 website compliance surveys in South Africa 'painted a bleak picture' of non-compliance and general indifference towards laws and regulations governing websites and the online sale of goods and services in South Africa". In 2002, 26% of South African website operators claimed that they were not aware of the compliance requirements, and this number increased in 2004 by 5% to 31% (Buys, 2004).

The failure to comply with the law, according to Buys (2004), has led to an increase in website crime: "During March 2002, a defamatory statement posted to the website of *Kick Off* magazine, ended in the High Court. A month later the *Department of Health* investigated an illegal online pharmacy in Table View and in June of the same year, the *Gauteng Metro Police* attempted to close down a website that warned motorists of speed traps around Johannesburg."

The problem was exacerbated by the fact that even after the promulgation of the Electronic Communications and Transactions Act No. 25 of 2005 (ECT Act), most South Africans did not comply with the requirements of of Chapter 7 and Part III of Chapter 3 of this Act (Buys Incorporated Attorneys, 2005).They did not seem to realise that failure to comply with the provisions of the law exposes their websites to serious risk and liability. Of the 1 550 websites surveyed by Buys Incorporated Attorneys (2004), the Telkom website (http://www.telkom.co.za) was the only one to score a full 100% compliance rate. Table 1.1 below reflects the summarised results of the 2004 South African website compliance survey (Buys Incorporated Attorneys, 2004).

Table 1.1: South African Website Compliance 2004

ASPECT SURVEYED	2002	2004
Total number of websites surveyed	607	1 550
Percentage of websites with legal notices at all	47.3%	81%
Percentage of websites with terms and conditions available as hyperlinks	7.1%	6%
Percentage of websites with liability disclaimers available as hyperlinks	3.8%	8%
Percentage of website operators who do not know what to do to become compliant	26%	31%
Percentage of website operators who understand the risks and liabilities of non-compliance	27%	43%
Percentage of website legal notices that address the provisions of Chapter 3, Part II and Chapter 7 of the ECT Act	5.06%	3.22%
Percentage of website operators who claim compliance is too expensive	66.3%	85.8%
Percentage of website operators who are likely to use affordable DIY compliance tools, if available	94%	87%
Percentage of websites that position and implement legal notices correctly	No results	9.3%
Percentage of website legal notices that are printable or saveable as required by section 11(3) of the ECT Act	No results	10.1%

Source: Buys, 2004

Other than the aforesaid website compliance survey conducted by Buys Incorporated Attorneys in 2002 and 2004, there has not been any substantial study that focuses on the compliance of information security related legislation by organisations in South Africa (Buys, 2004). Moreover, it remains to be established whether the existing company policies are in line with the national and international legal regime. The lack of results with regard to consideration of legal and policy aspects in the South African corporate environment seems to indicate the need for research in this field. There is a gap in the literature as to how information security legal policy and legislation add value to the corporate environment not just within the South African corporate context, but also internationally. Current literature does not indicate whether South African organisations are complying with the national legal and policy framework regarding information security.

1.4 RESEARCH QUESTION AND OBJECTIVES OF THE STUDY

Within this context, the main research question was formulated as follows:

Are South African companies employing legal prescriptions to enhance information security and how are they doing it?

In order to answer the research question, it was necessary to answer the following sub-questions:

1. To what extent are organisations in South Africa integrating information security legal requirements into their policy formulation and implementation?
2. To what extent are organisations in South Africa implementing information security policies in which the legal aspects have been integrated?

The abovementioned research question and sub-questions were answered by employing various data collection methods.

1.4.1 Objectives of the study

The aim of the study was to assess how South African companies integrate legal and policy aspects when they deal with information security issues. In order to attain the set aim, the objectives were outlined as follows:

i. To undertake a study of the literature to determine:
   - the nature of information security related problems; and
   - the relevant South African laws pertaining to information security.

ii. To determine by means of the field study the following:
   - the way in which the South African companies are employing legislation imperatives in providing information security;
   - the extent to which the South African legal framework impacts on the formulation of information security policies at organisational level; and
   - the extent to which South African companies are complying with the commercial websites legal requirements.

iii. To determine by means of studying documents (policies, procedures and strategies) collected from the participating companies how they are aligning their information security measures with legislation and policies.

iv. To suggest a concept model of legal compliance for information security in the corporate environment within the South African context.

1.5 BRIEF OVERVIEW OF THE RESEARCH DESIGN AND METHODOLOGY

This study employed a generic qualitative approach with document analysis, website analysis, and key informant interviews being used for data collection purposes, apart from the literature review. Qualitative analysis methods were used to analyse the collected data. Participants in this study were 45 South African organisations. The study involved companies from different industrial sectors such as banking, transport, online retail, hotel, broadcasting, and telecommunications, and included the energy, mining, insurance, banking, telecommunication and services industrial sectors.

Convenience and purposive sampling were used to select the participating companies. The trustworthiness of this study, amongst other things, was guaranteed by using both internal and external validities.

The researcher used data collection methods to identify the causal link between policy aspects, legal aspects and information security in the South African corporate environment. The research methodology used in this study is explained in Chapter 4.

1.6 SIGNIFICANCE OF THE STUDY

This study is intended to provide important insights into the future application of legal and policy aspects in the provision of information security in the South African corporate environment. Companies, boards of directors, ICT executives, information security practitioners, e-commerce participants, and policy formulators may use the findings of this study as a resource and guide. It is envisaged that the findings and recommendations of this study will be transferable and applicable to other contexts and countries. The study contributes both theoretically and practically in the area of compliance with legislation when implementing information security.

The originality of the contribution of this study to the academic and industry knowledge-base of information security benefited from additional contextualised corporate descriptions that add to the understanding of the complexities of employing legislation to enhance information security in the South African corporate environment. This study produced the Concept Model of Legal Compliance for Information Security in the Corporate Environment. This model embodies the contribution of the study. The fieldwork of this study produced adequate empirical evidence and the importance of the Concept Model was illustrated within the discussion framework of this thesis to convince information security practitioners and experts that the proposed Concept Model has the inherent capacity and integrity to become a recognised corporate practice in the field of information security.

Although this study focused on the legal aspects to consider when providing information security in organisations, it is important to clarify that this is not a legal study, but rather information system research. Furthermore, the principle of IANAL (I am not a lawyer) is applicable to this study.

1.7 STRUCTURE OF THE THESIS

Chapter 1 provided an introduction, overview of, and general orientation to the study, the rationale and aim for conducting the study, the research question and sub-questions, potential contribution of the study, the research programme and a summary of chapter 1. The next two chapters contain literature review – Chapter 2 focuses on information security and Chapter 3 on the South African legislation pertaining to information security.

Chapter 2 contains a descriptive outline of information security history, risks, threats, and crimes. For the purpose of this study, the following information security issues will be dealt with – hacking, viruses, privacy, ethical issues and industrial espionage.

Chapter 3 specifically provides a legal framework for information security in South Africa. This includes the topical issues which are covered in the Constitution of the Republic of South Africa; as well as other relevant pieces of legislation.

Chapter 4 focuses on the research design of the study. Details of the research approach and procedures are supplied, including details about participants in the research and sampling, data collection methods and analysis techniques.

In **Chapters 5 and 6** the analysed data and findings of the study are reported against the background of the literature review and the research questions. The analysis has shown that the participation of the board of directors in the development of information security policies was minimal; most information security practitioners were not familiar with the legal and policy aspects that they were supposed to integrate with the implementation of information security and thus most organisations were not complying with the law.

Chapter 7 contains the Concept Model of Legal Compliance for Information Security in the Corporate Environment. The Concept Model embodies the contribution of the study. This chapter provides a model whereby legal requirements are incorporated into the information security endeavours. The Concept Model is the intellectual property of the researcher and can be seen as a synthesis of theory, practice and cognitive perspectives gained over years of practical experience.

Chapter 8 presents a summary of the whole study, the conclusion, recommendations for further study and recommendations to the policy makers and industry.

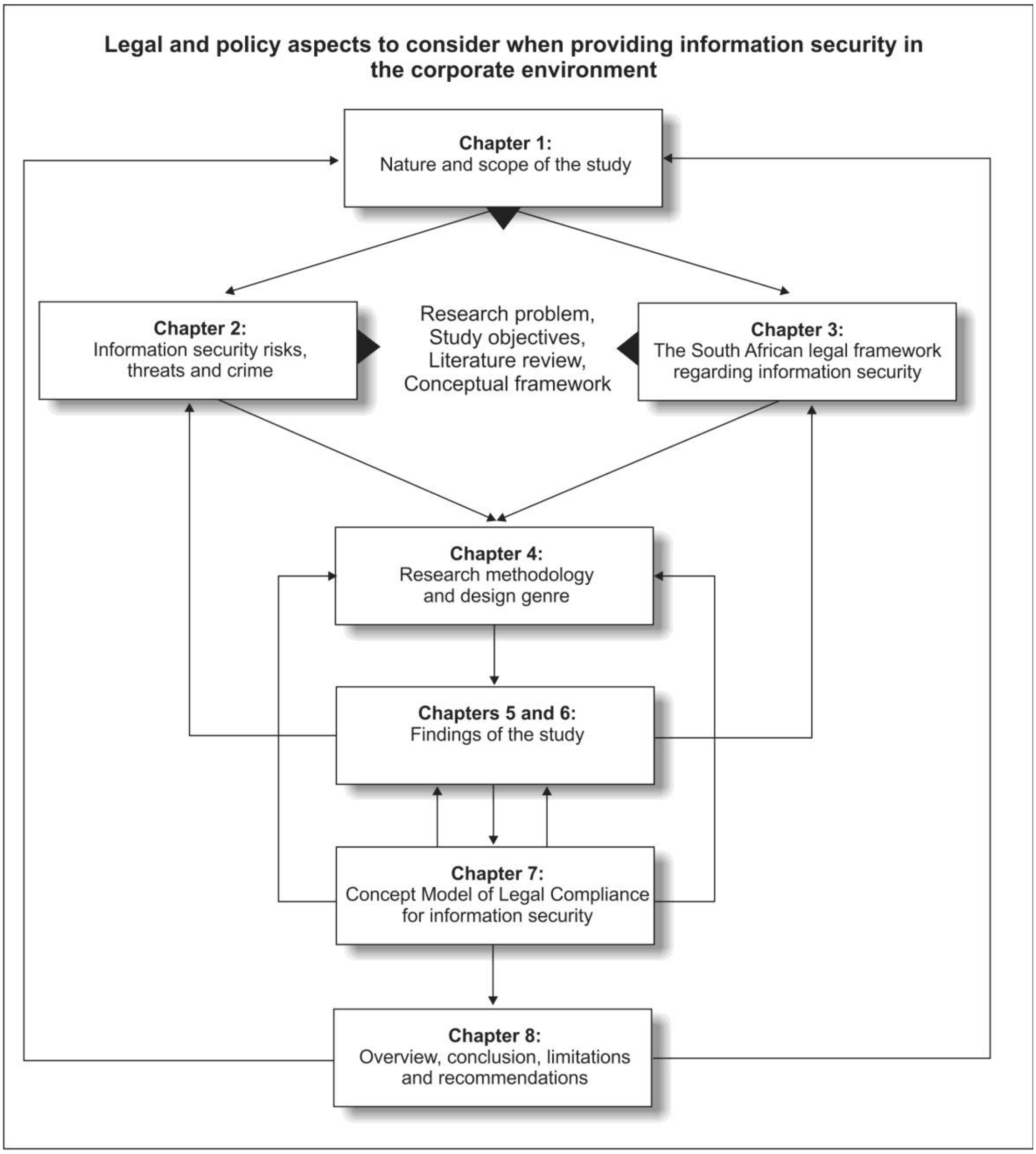

Legal and policy aspects to consider when providing information security in the corporate environment
Chapter 1:
Nature and scope of the study
Chapter 2:
Information security risks, threats and crime
Research problem,
Study objectives,
Literature review,
Conceptual framework
Chapter 3:
The South African legal framework regarding information security
Chapter 4:
Research methodology and design genre
Chapters 5 and 6:
Findings of the study
Chapter 7:
Concept Model of Legal Compliance for information security
Chapter 8:
Overview, conclusion, limitations and recommendations

Figure 1.1 Relationship between the various chapters.

The thesis concludes with a list of references consulted and appendices.

1.8 SUMMARY

Most organisations around the world, as in South Africa, use the Internet for business related transactions. The use of the Internet for business purposes is called e-commerce. As explained in Section 1.2 of this chapter, e-commerce is not immune to risks, threats and crime. Organisations should therefore provide information security to protect online merchants and consumers. On the other hand, Section 1.2 also indicated that the responsibility of protecting online merchants and consumers cannot be left only in the hands of the corporate sector, and thus governments, regional and international organisations should also play a role. The perception that the Internet is an unprotected business medium leads to doubts amongst electronic shoppers to embrace e-commerce. These kinds of doubts tend to directly or indirectly negatively affect economic development. Notwithstanding this, there are a number of organisations that are succeeding in e-commerce. This could, at least in part, be attributed to their reputation for providing satisfactory information security. Section 1.2 also showed that the companies that succeed in e-commerce are those that implement information security policies. These policies are on their websites for the attention of Internet consumers and business partners. In most instances, these policies deal with security and privacy related issues.

The background section has explained the significance of international and national legal frameworks in the provision of information security. Companies that want to succeed in e-commerce should, amongst other things, go beyond technical security measures by employing policy and legal aspects of information security. Based on the literature, it is the view of the researcher that technical measures should be applied within a particular organisational, national and international policy and legal framework.

It was indicated in the section on research design that the researcher used data collection methods to identify the causal link between policy aspects, legal aspects and information security in the South African corporate environment. The literature also discussed the legal framework of information security in South Africa. This study investigated how this legal framework and South African organisational policies are applied at company level as measures to provide information security.

Section 1.3, which deals with the problem statement, provides the rationale for this study. The literature does not show how the legal and policy aspects are used in the provision of information security in South Africa. The section also shows the research question and sub-questions. It was stated that the aim of this study was, amongst other considerations, to provide important insights into the future use of legal and policy aspects in the provision of information security in the South African corporate environment. It was stated that the findings and recommendation of this study are transferable and applicable to other contexts and countries. Chapter Two, the first of two literature review chapters, provides a descriptive outline of information security history, risks, threats, and crimes.

CHAPTER TWO

INFORMATION SECURITY RISKS, THREATS AND CRIME

2.1 INTRODUCTION

Individuals and organizations need to protect their information from attackers or competitors as loss of information could lead to lawsuits or loss of business. Simply put, information should always be protected and secured. According to literature, Information Security refers to "measures adopted to prevent the unauthorized use, misuse, modification, or denial of use of knowledge, facts, data or capabilities" (Maiwald, 2004:4). The aforesaid statements are supported by authors such as Wu and Ye, (2014) and Mukundan and Sai (2014). In other words, Information Security comprises the preventative measures put in place to protect information and capabilities, keeping these safe from threats and any exploitation (*ibid*). The field of information security is usually inter-related with other fields such as computer security and information assurance. These, though some subtle differences may exist between them, are characterized by the common aims of ensuring the confidentiality, integrity and availability of information (Westby, 2013).

Society, technology and information security have evolved over time. Therefore, the effectiveness of guarding information today requires an understanding of how information security has been handled in the past (Westby, 2013). Cassim (2012) postulates that Information Security breaches have increased dramatically in the past few years. The attacks are becoming increasingly more sophisticated as the field of computer and network technology evolves. This chapter outlines a brief history of information security.

This chapter provides broad insights on information security history, risks, threats and crime. It was mentioned in Chapter 1 that the overall purpose of this study is to assess how organisations can, amongst other things, use legal and policy aspects to address their information security concerns. The legal and policy aspects pertaining to information security do not occur in a vacuum and thus a broader understanding of issues that constitute information security risks, threats and crimes is essential. For the purpose of this study, the following information crimes will be dealt with: hacking, malicious code or viruses, privacy and ethical issues and social engineering. These are briefly defined below.

Hacking is one of the most well-known types of information security related risks and crimes (Maiwald, 2004; Adrian, 2013). Simply put, hacking involves breaking into information systems in order to make them dysfunctional or to steal information for whatever purpose. It is indicated in this chapter that there are numerous causes for hacking. This chapter also points out historical hacking techniques, such as open sharing, distributed attacks and kernel-level Rootkit. Technical protective measures to deal with hacking are also discussed in this chapter.

Malicious code, widely known as malware or viruses, is one of the major information security related problems (Isaacs, 2013). It is demonstrated in this chapter that just as in the biological field, it is difficult to contain computer viruses. Malware has the ability to destroy information systems. An historical overview of malware is presented in this chapter. Some authors, such as Kehe and Schichao (2014) claim that viruses existed before the 1980s. This claim is, however, contested by authors like James, Nottingham and Kim (2013). It was found that during the early 1990s, malware authors improved them in such a way that it became very difficult to detect them. Types of malware and measures to deal with them are explained.

This chapter also reflects on the ethical issues in the context of information security and the defence mechanisms to eradicate these. Ethical issues include social engineering, privacy, and copyright matters. The last part of this chapter reflects briefly on information security policies.

2.2 A BRIEF HISTORY OF ECOMMERCE AND INFORMATION SECURITY CONCERNS

This section provides an overview of the history of e-commerce by reflecting on the emergence of the Internet and World Wide Web. It also deals with electronic payments and information security challenges.

2.2.1 The emergence of the Internet and World Wide Web

Richardson (2000) reported that the Internet started from humble beginnings as a USA government military project. Nowadays, the Internet is one of the dominating communication and commercial tools in the corporate world. The Internet came into being during the Cold War in the 1950s. The USA military was concerned about the potential of a nuclear attack that could destroy all their military data and information (Richardson, 2000). It is on this premise that the Department of Defence worked with the Rand Corporation in dispersing their computers geographically. These computers were networked together and no one computer would be in charge of all the data (Chance-Hill & Odell, 2014; James et al., 2013). A message sent to another networked computer was labelled with the receiver's address. Lawrence, Newton, Corbitt, Lawrence and Tidwell (2000) had noted that during the early days of the Internet, its activities were subsidised by the government and strictly kept out of reach of the business community.

According to Moschovitis, Poole, Schuyler and Senft (1999) and Flanagin and Metzger (2014), the use of the networked computers has since then grown beyond the military. The corporate sector and private citizens started to use the Internet for communication and commercial purposes. In fact, according to Lawrence et al., (2000), in the 1960s some private people in USA were already using a forerunner of the Internet as we know it today. However, it was only in the 1990s that the Internet started to make its mark in communication, research and increasingly, to sell goods and services online. The Internet has moved through four waves. These waves are reflected in Table 2.1 below.

Table 2.1: Four waves of the Internet development

Wave	Countries	Characteristics
Wave 1	United States, Canada and the Nordics	Characteristics by early adoption in the universities and government in the 1980s. These countries are among the heaviest commercial users of the technology.
Wave 2	The rest of the European Union, Australia, New Zealand, Japan, Republic of Korea, Taiwan, Singapore, Hong Kong and Israel	Characterised by high level of private and public sector interest in developing broad information societies. Extensive commercial uses although focus on consumer applications varies widely.
Wave 3	Developing countries across South East Asia, China, Brazil, Argentina, South Africa, Egypt, and smaller islands states such as Tonga, Fiji, Barbados and French Polynesia	Characterised by high levels of interest in initiating and developing business applications of online commerce.
Wave 4	Least developed countries or other countries that deliberately shun Internet use.	Characterised to date by unattractive investment environment. In some countries there have been attempts to ban the Internet for political and social reasons.

Adopted from Lawrence et al., (2000:2)

Although Table 2.1 does not show the years in which particular waves happened, it provides important insights regarding the history and background of the Internet and e-commerce. Lawrence et al., (2000) wrote that in the mid-1980s, the National Science Foundation (NSF) developed a high speed, long-distance telecommunications network into which other networks could be connected. This network is currently supported by other organisations. By 1991, the NSF removed its restrictive usage policy and allowed the business community to have commercial sites. This led to the arrival of the World Wide Web (WWW) (Moschovitis et al., 1999). Although in this study, the terms Internet, WWW, Web and Cyber will be used synonymously and interchangeably, it should be noted that the WWW is just one of the services offered by the Internet (Shipps & Philips, 2013; Kehe & Shichao, 2014). The WWW has grown rapidly since its inception in the 1990s.

The arrival of the WWW encouraged business interest in the Internet (Porrini, Palmonari & Vizzari, 2014). The Web is a graphical hypertext environment, which functions within the Internet. It consists of global collections of electronic documents that have hyperlinks connected to related documents (Elmalech & Sarne, 2014). The WWW supports or/and incorporates multimedia (audio and visual) presentations, text and graphics. Lawrence et al., (2000:4) reported that the protocol (rules, procedures and standards) that is employed by the Web is the “hypertext transfer protocol” (http), whilst the protocol for commercial activities on the Web is secure hypertext transfer protocol, which creates the basis for “secure communications, authentication, digital signatures and encryption”.

Nowadays, the use of the Internet for commercial purposes is still growing rapidly (Abdullah, Xu & Geva, 2013). This is matched by the consumers' accessibility to the Internet (Lostorto, 2013). Lower computer prices and easy Internet access are encouraging people to visit business Web sites. Customers and prospective customers can now visit business Web sites more frequently (Bedard, 2014). This is enhanced by the fact that surfing the Internet is becoming a habit amongst people which has led to both print and electronic media developing Web sites for regular news updates and breaking news.

2.2.2 The emergence of electronic transactions

Lawrence et al., (2000:6) reported that the use of e-commerce in the financial services industry started in the early sixties. These include the automation/computerisation of cheque processing, credit card processing, and wire transfers (Porrini, Palmonari & Vizzari, 2014). This trend, according to Collin (1998), was followed by banking teller stations in local branches, which were automated to allow direct processing of certain transactions. The automation of teller stations enabled customers to have direct access to their account information (Stampler, 2013).

In the 1990s, personal computing was extended from the office to the home and thus the business sector started to extend their technology to bring services to customers at their homes (Lawrence et al., 2006). The merchants found electronic transaction was a great cost-saver while on the other hand their revenue sources were increasing (James & Rajendran, 2013). According to Flanagin and Metzger (2014), the business sector also realised that electronic transactions made them more competitive in customer service and customer retention.

According to Lawrence et al., (2000:7), there are four critical issues that have impacted the speed of e-commerce evolution. These include the following:

- the need for improved technology to ensure the security of the transaction;
- the availability of a variety of payment protocols;
- system reliability for twenty-four hours a day seven days a week operations, and
- the flexibility of the platform to absorb new capabilities as they become available.

Lawrence et al., (2000) and Washah (2013) reported that *electronic data interchange* (EDI) and e-mail has been used for many years for commercial electronic transactions. It was also used for work flow and re-engineering applications (Elmalch & Sarne, 2014). It is on this premise that towards the end of 1999, American Online already had about 20 million subscribers (Fang & Qureshi, 2014). EDI was eventually used in conjunction with the Internet. As a result, some companies that did not use the Internet for business purposes started losing contracts and customers at the beginning of the 21st Century (Costante, Paci & Zannone, 2013).

Lawrence et al. (2000) reported that throughout the recorded commercial history of humankind, people have engaged in the exchange of value in many ways. In earlier times, people acquired goods and services by exchanging tokens of various sorts (Mathiesen, 1997; Chance-Hill & Odell, 2014). This was referred to as bartering. It is only two or three millennia ago that the first coins with specific value were introduced. These primitive coins formed the basis of the modern forms of money. In fact, today, people can engage in the exchange of services and goods in various ways other than coin and paper money. This should be attributed to the inception of electronic forms of money (Mathiesen, 1997; Flanagin & Metzger, 2014).

Lee (2012) reported that since the early 1990s, the Internet has grown rapidly in terms of the quantity of both users and applications. On the other hand, merchants and consumers have noted the endless commercial potential of the Internet and thus commercial transactions emerged on the Internet (Shipps & Philips, 2013). One should be quick to indicate that whilst agreement to sell and buy was conducted via the Internet, payment tendered would be arranged outside the Internet (Elmalech & Sane, 2014). This would be done by resorting to conventional ways of paying (Lostorto, 2013). The avoidance of using the Internet for electronic payment should be attributed to concerns regarding information security and privacy (Bedard, 2014). According to Stampler (2013), it was really unsatisfactory to add another step of paying through a different medium of communication before the transactions could be finalised.

To date, much effort and resources have been put into the establishment of security in the Internet to address the concerns of the merchants and consumers (Stampler, 2013).

Contemporary lawmakers have encouraged payment with paper-based methods, but lately they are increasingly allowing electronic alternatives (James & Rajendran, 2013). Policy formulators agreed to this transactional method after recognising that uniformity among countries was essential to facilitate e-commerce (Washah, 2013). Electronic payments include electronic cards, credit cards, debit cards, digital cash, and other digital currencies (Elmalech & Sarne, 2014).

2.2.3 Information security issues: implications for e-commerce

It has been stated in the preceding sections that e-commerce is growing fast. It does seem however, that one of the major obstacles to a more rapid growth of e-commerce has been the customer concerns regarding information security related issues (Fang & Qureshi, 2014). It should also be noted that, from the start, the Internet was designed to share information – and not to hide it (Elmalech & Sarne, 2014). At that stage it did not seem to be necessary to build in tight information security features since it was taken for granted that all transmissions would be carried over private lines. In fact, top secret military transmissions are still on private networks, but the basic technology has moved to the world's public network – the Internet and companies' internal networks (Washah, 2013). It is here that consumers and merchants find themselves using insecure protocols which were primarily designed for connectivity and information security – going over inherently unprotected public and corporate networks where there is a serious "lack of sentries guarding the gates" (Crume, 2000).

A major concern in e-commerce has been information security for confidentiality, integrity, and availability:

Information security for confidentiality: It has been stated in this section that credit and debit cards are some of the electronic payment methods in e-commerce environment. One of the major impediments to the general use of these cards as a means of payment for the e-commerce transactions has been the concern in some consumers' thinking that they lack sufficient confidentiality (James & Rajendran, 2013)

Information security for integrity: Bedard (2014) wrote that one of the problems of using the Internet for commercial purposes is its questionable integrity. It is here that some marketers find it difficult to convince consumers to buy their products and services online (Elmalech & Sarne, 2014). On the other hand, some consumers would not even bother to consider an online advertisement due to the integrity concerns. This has led consumers to only trust established online retailers like Amazon.com and Kalahari.Net (Shipps & Phillips, 2013). The consequence of this is that small, micro, and medium enterprise end up suffering huge losses.

Information security for availability: One of the major challenges facing online retailers is to secure the availability of their e-commerce Web sites consistently (Chance-Hill & Odell, 2014). The unavailability of a particular Web site could be due to an attack (Flanagin & Metzger, 2014). According to Fang and Quresh (2014), attacks on availability are designed to forbid legitimate users from using an online resource, such as Internet banking.

The above paragraphs have dealt with information security challenges that are confronting e-commerce globally and South Africa, in particular. Whilst there are technical remedies that could address the information security challenges, this study will argue that policy and legal aspects should be used to mitigate these problems.

2.3 OVERVIEW OF INFORMATION SECURITY RISK, THREAT AND CRIME

A chapter on information security risks, threats and crime would be incomplete without a section on hacking. According to authors such as Kamel and Lanet (2013), a hacker is a person who breaks into computers and/or its systems. Abdulla et al. (2013) notes that the term hacker has many definitions, starting from a corporate systems administrator who is able to make computer systems work. The authors note that the term has been co-opted by the media and “stripped of its meaning”. This word used to be considered complimentary in the past rather than being an insult (*ibid*). Some authors report that the word ‘hacker’ is a derogatory term (Maiwald, 2004; Abdulla et al., 2013). Maiwald (2004) argues that perhaps the more appropriate term would be “cracker” or “criminal”. Nevertheless, to comply with the current general usage and due to its derogatory meaning, the term “hacker” will be used in this study to identify those people who intrude into computer systems and/or make such systems dysfunctional, and will include crackers.

2.3.1 Historical hacking techniques

An understanding of the hackers' motivation is the key element to understand hacking. The purpose and motive of hacking are interlinked. Maiwald (2004) reasons that understanding the motivation enables us to understand what makes the computer and networks interesting to the hacker: "Is the system somehow valuable or enticing?" Answering this and other questions enables information security professionals to better assess the vulnerability of their computer systems. They will also be able to determine how they could use technical, policy and legal measures to protect their systems. Several authors assert that hacking is motivated by challenge, greed, malicious intent, crime, industrial espionage, press, policy and terrorism (Nye, 2013; Pisaric, 2013, Thaanum, 2013). This section provides an historical overview of the hacking techniques showing the evolution of techniques used by hackers.

Open file sharing

When the Internet was initially established, according to Maiwald (2004) and Xiong (2013), it was a platform of information sharing and collaboration amongst research institutions. It is on this basis that most usage of computer systems was confined to the sharing of information. Maiwald (2004) provided an example of the UNIX systems – it allows a computer to mount the drives from any another computer across the network. This is also applicable to the Internet and Local Area Network (LAN). File sharing via the Internet, Network File System (NFS) and LAN was used by some of the first hackers to infiltrate systems (Martin & De Andrade, 2013).

Maiwald (2004) reports that NFS utilised user identity numbers to allow access to the drive that contains information: "So if a file were limited to a user Joe with user identity 104 on its home machine, another user Alice with user identity 104 on a remote machine would be able to read the file. The danger associated with that was that some systems allowed the sharing of the root file system and the hacker could change the configuration files of that particular remote system (Maiwald, 2004; Thompson, 2014). Most operating systems have now been improved to avoid this.

Distributed attacks

One of the trends in the evolution of hacking is the move towards distributed attack architectures (Skoudis, 2004; Xiong, 2013). The hackers are maximising the distribution ability of the Internet itself to enhance their hacking capabilities. The hacker takes a traditional system attack and divides the work amongst several computer systems (Maiwald, 2004; Martin & De Andrade, 2013). Most systems are collaborating and thus the hacker's probabilities for success are good. It is still very difficult to detect and/or trace a hacker who uses distributed attacks. Poorly protected systems in government departments, learning institutions, companies and homes with Internet connectivity are easy targets for a hacker. According to Skoudis (2004), these hackers use, "automated vulnerability scanning tools, including home-grown scripts and freeware tools such as the Nessus Vulnerability Scanner, amongst many others, to scan large swathes of the Internet".

Kernel-level Rootkit

Hackers are not just attacking major protocols such as address resolution protocols and domain name service (DNA); they also target the "heart" of an operating system (Skoudis, 2004; Agwu, 2013). The subsections below detail the evolution of kernel-level Rootkits as espoused by Skoudis (2004).

(a) Traditional Rootkits

A traditional Rootkit is a set of hacking tools that enables the hacker to obtain super-user access on a computer system (Skoudis, 2004; Alazab & Venkatraman, 2013). Once the hacker obtains root-level control on a computer, the Rootkit allows the hacker to maintain that access. Traditional Rootkits would normally include a backdoor so that the hacker could get into the system and penetrate the normal information security defence. It is recorded that traditional Rootkits create backdoors and hiding techniques by substituting important executable programmes included in the operating system (Mohite & Kumthekar, 2013).

(b) Kernel-level Rootkits

Whilst traditional Rootkits substitute critical system executables, hackers have gone a step further by implementing kernel-level Rootkits (Skoudis, 2004). The kernel is the heart of many operating systems, regulating access to resources such as the computer disk, system processor and memory. Kernel-level Rootkits change the kernel itself rather than just tampering with application-level programmes (Lawande, 2012).

Most common capabilities of kernel-level Rootkits are execution redirection and file hiding. Each of the kernel-level Rootkits' capabilities is very powerful on their own and thus they provide a hacker with the ability to totally modify the machine at the hacker's whim (Lawande, 2012). It is more difficult to create defences against the traditional Rootkit than the kernel-level Rootkits. The tracing and detection of the kernel-level Rootkits is usually difficult (Huey, Nhan & Broll, 2013). This should be attributed to the fact that getting into the system depends on the hacker-modified kernel. The next section deals with measures to tackle malicious code.

2.3.2 Malicious Code as information security risk, threat and crime

The world is confronted by the fast growth of computer viruses and it is difficult to address the impact of these viruses, similar to biological viruses (Slade, 2004; Williams, 2013). Slade (2004) reports that, due to the rapid evolution in the corporate and biological world, IBM's computer virus research task team has investigated possible similarities and differences between biological and computer viruses and epidemiology extensively. The researchers found that the evolution of computer viruses is faster than their biological counterparts. Slade (2004:1259) attributes this to the huge growth of computer technology, "as well as homogenisation of computers, operating systems, and software". This aforesaid statement is supported by Bedard (2014).

Malicious code/software is an information security problem for most organisations, institutions, government departments and individual home users (Ceccagnoli, Forman, Huang & Wu, 2012). According to Maiwald (2004:67), the term "malicious code" refers to computer viruses, Trojan horse programmes, worms and others. Together they are called *malware* (Cecere & Rochelandet, 2013). Malware is a relatively new term in the ICT field and was coined to describe software programmes that are deliberately created to penetrate a system, breaking security, carrying malicious or destructive payloads (Cecere & Rochelandet, 2013; Ceccagnoli et al., 2012). The term malware is sometimes used loosely as a synonym for virus, whilst the word virus is sometimes used simply to refer to any type of computer problem.

Cecere and Rochelandet (2013) declared that viruses are the biggest group of malware, both in terms of quantities of entities and their impact on the information security field. Viruses will therefore receive more attention in this section but will not be the only type of malware reviewed. It should also be noted that once the attacker launches a malware attack, it will continue to attack without reference to the attacker or user, expanding the attack to other computer systems (Cassim, 2012). It is on this premise that Slade (2004) argues that there is a qualitative difference between malware and the hacking toolkits, or scripts, which are supposed to function under the hacker's control.

2.3.3 Historical overview of malware

According to Slade (2004) and Cassim (2012), many claims have been reported regarding the existence of computer malware before the 1980s. However, these claims lack evidence or are directed to entities that can be regarded as a virus under the loose definition of the term. Slade (2004:1259) reports that the Core Wars programming contests included self-replicating code. In fact, other types of malware have been known since the invention of computers.

Two Apple II viruses were reportedly created in the early 1980s. According to Slade (2004), Fred Cohen's leading scholarly research conducted during the course of that decade provided some evidence that the first malware that attacked successfully was developed in the 1980s. Schneier (2000) reports that in 1983, a certain student named Fred Cohen authored the first computer virus. He reportedly did it to make a point after realising that most people did not believe it was possible to have a computer virus. According to Schneier (2000), some IT experts then started to copy him, most of them just to provoke the world. It is estimated that there are more than 150 000 different viruses in circulation and more than 148 000 computers compromised daily (Tiwari, 2013). In the 1980s, the only available malware was boot-sector viruses and file infectors. This malicious software spread very slowly, largely disseminated on floppy disks, and was slow to distribute geographically (Slade, 2004; Adrian (2013). However, during the early 1990s, malware authors began to improve malware so that it would be difficult to detect and easier to spread via networks.

Slade (2004) recalls that in the middle of the 1990s, macro and script malware in the wild were introduced. Macro viruses also created new variants rapidly because the malware carried their own source code. In the late 1990s and early 2000s, the e-mail virus became a major force in information security. E-mail viruses grew extensively by spreading themselves worldwide within a short space of time. According to Slade (2004:1259), some versions of malware would reproduce copies of themselves to such an extent that organisations' mail servers became dysfunctional. The subsequent convergence of technologies has led to the creation of malware with a greater capacity for destruction (Brenner, 2013). The next section provides broad descriptions of malware types.

2.3.4 Malware types

As previously explained, viruses are not the only type of malware. Other forms of malware include worms and Trojans. Brenner (2013) and Slade (2004) advise that some types of malware include qualities of more than one class and it is therefore difficult to draw any distinctions pertaining to individual examples. There is also an increase in the convergence of malware.

Viruses

Schneier (2000:152) uses a metaphor to describe a computer virus: "A biological virus is a simple sub-microscope infections agent that often causes disease in plants, animals, and humans. It consists essentially of a core of RNA or DNA surrounded by a protein coat. Viruses are unable to replicate without a host cell, and are typically not considered living organisms". For once, this metaphor is a true reflection of its meaning. A computer virus is a computer programme which embeds itself to another computer programme (Bin-Baba, Tamjid & Gholipour, 2013).

Adrian (2013) reports that a computer virus is a programme/code/software which is written with the capacity to replicate and spread itself, without the knowledge and consent of the computer system user. Slade (2004:1260) defines a computer virus as, "a programme that modifies other programmes to contain a possibly altered version of itself". Nye (2013) claimed that virus's use the resources of the host of the computer or system to duplicate themselvesand disperse without instructions of the operator or author. Viruses have the ability to attach themselves to other programmes as an infection (Bin-Baba et al, 2013). However, viruses can also attach to an object without the intervention of the user. According to Slade (2004:1260), the object can be an, “e-mail, programme file, document, floppy disk, CD-ROM, short message system (SMS) on cellular telephones, or any similar information medium”.

Pisaric (2013) and Slade (2004) stress the fact that a virus should be distinguished by its capacity to reproduce and spread. Lawande (2012) is quick to point out that a virus is not simply anything that goes wrong with a computer. It has also been stated in preceding paragraphs that a virus is not merely another type of malware. For example, Trojan horse programmes and logic bombs do not have the ability to reproduce themselves (Latimer, 2013). Viruses and worms are distinguished by the fact that the viruses need an action (not instructions or command) of the user to trigger reproduction and distribution (Williams, 2013). The actions of the user in this instance are not deliberate instructions or commands to the virus, but rather the usual general computer actions.

According to Maiwald (2004) and Agwu (2013), a virus is a programme that piggy-backs on other executable programmes. Viruses are not designed to live by themselves. It is on this basis that when a programme that is infected by a virus is executed, the virus becomes executed and carries out its actions. Wu (2013), Wu and Ye (2014) observed that the users do not always realise the implications of their actions. Slade (2004) supports this reasoning by declaring that sometimes users are helping the virus.

Viruses have the ability to modify systems and applications. Other types of viruses are malicious and erase files (Thaanum, 2013). They also have the capacity to make the systems and applications redundant. However, certain types of virus are not malicious except that they disperse themselves to other systems (Maiwald, 2004; Latimer, 2013). Some of the changes caused by a virus have negative input to the virus themselves. Schneier (2000), and Nikolayevich and Borisovna (2014) have noted that modifications in the underlying computers impact on the ability of the virus to function and it dies.

There are different forms of viruses. The differences do not necessarily reflect a high degree of distinct division. For example, according to Slade (2004), a file infector may also infect the system. It is also difficult to determine a strict division between macro and script viruses. Examples include File infectors; Boot-sector infectors; System; Companion; E-mail; Multipartite; and Script viruses (Slade, 2004). This assertion is supported by authors such as Demirkan and Delen (2013), and Wu and Ye (2014).

Trojan Horses

Slade (2004) and Behr (2013) claim that apart from viruses, Trojans, or Trojan horse programmes are the second largest form of malware. Maiwald (2004:68) observes that just as the ancient Greeks used a gift to conceal evidence of their attack, the Trojan horse programme similarly conceals its malicious nature under the pretext of something useful or interesting.

Schneier (2000:155) provides a reminder of the original Trojan horse: "The Greeks besieged Troy for ten years, and it was showing no sign of falling. Out of desperation – and probably boredom – Odysseus had the Greek soldiers build a large wooden horse and put some of them inside. He left it for Trojans as an admission of defeat and then told his army to pretend to sail away, trying not to giggle as they did. The Trojans took the wooden horse inside the walls – every artist's rendition puts the horse on a wheeled platform – despite the better judgement of their priests. That night, the Greeks crept out of the horse, opened the gates, and let the rest of the Greek army inside. The Greeks then massacred the Trojans, looted their wealth, and burned the city." This is a widely accepted story, although its authenticity cannot be proven, but it provides an understanding of how the Trojan horse virus operates (Stantchev, Petruch & Tamm, 2013).

According to Wu and Ye (2014), a Trojan horse is a malware programme attached to a genuine piece of software, structured to mislead the user into thinking that it is not harmful. Technically, a Trojan horse is a code that secretly inserts itself into the user's machine, analyses the user keyboard buffer until it discovers what seems to be a credit card number – "right number of digits, checksum matches – and sends that number via TCP/IP" to the attacker (Schneier, 2000:156). Morrison (2013) claims that Trojan code has the ability to identify usernames and passwords and convey these to their sender. In a very subtle way, they can modify the user or host's encryption programme to select keys from a small random pool, thus weakening the key space (Ifinedo, 2014; Stantchev et al, 2013).

Abawajy (2014) observes that the most difficult part for the potential attacker is getting the Trojan horse secretly into the computer of the victim. Sometimes a hacker breaks into the victim's office and puts the Trojan horse in his/her computer. Some hackers may go to the extent of persuading someone to install it on his/her computer (Schneier, 2000; Mbaku, 2013). However, Slade (2004) notes that some Trojans can be installed remotely. This claim is supported by Li, Zhang, Chu, Suzuki and Araki (2012).

Worms

A *worm*, as the name implies, is a malware programme which 'crawls' from system to system via networks without any help from its targeted victims (Malware, 2004:68). This assertion is supported by Mohite and Kumthekar (2013) who note that a worm disperses and replicates on its own. All that is required is for the author of the worm to get it going. The first recorded type of worm was a popular Internet worm authored by Robert Morris in 1988 (Malware, 2004; Li et al., 2012). The Morris Worm was structured to exploit several computer system weaknesses, including poor passwords. In 1988, the Morris Worm crashed 6 000 computers which at that time comprised 10 percent of the computers linked to the Internet.

The worm exploits the system weaknesses to search systems in the Internet to manipulate and penetrate (Sowan & Jenkins, 2013). Once it settles into a system, it starts looking for additional victims. The convergence of technologies provides worms with a platform to launch attacks (Slade, 2004; Lin, 2012). The next section deals with information security ethical related issues.

2.4 ETHICAL ISSUES PERTAINING TO INFORMATION SECURITY

Ethical issues in information security include, but are not limited to social engineering, priracy and copyright. Only these three issues will be discussed because of their direct relationship with legal aspects that are relevant to this study.

2.4.1 Social engineering as an information security risk, threat and crime

According to Berti and Rogers (2004:147), social engineering is the term that originated in the field of social control, and that, "a social engineer can refer to the process of redefining a society or more correctly, an engineering society – to achieve some desired outcome". Radha and Mimal (2012) define social engineering as a process of trying to manipulate people's behaviour in a predictable manner, in order to get them to comply with the requirements of the manipulator. Vijaya (2013) observes that in information security, social engineering refers to endeavours to influence a system's host or user into either disclosing or acting in a way that will enable the intruder to obtain unauthorised access to, unauthorised use or unauthorised revelation of a computer system, network or data.

From the above definitions, one can conclude that social engineering is somehow synonymous with deception. In information security, it would mean deceiving the system host or user (Lin, 2012). According to Berti and Rogers (2004), deceiving someone is an old phenomenon in the history of crime, but is still very effective. Social engineering tends to attack the person's intelligence or inherent kindness. It is on this basis that the victims of social engineering do not want to admit to having been deceived because it makes them look stupid or unhelpful. The reluctance to divulge being deceived has led to the lack of proper statistics regarding social engineering in the field of information security (Lin, 2012). Nonetheless, many computer-related criminals have used social engineering rather than any other technical means to attack or intrude on information systems. The following paragraphs detail the factors that enable social engineering to succeed.

Factors that make social engineering succeed

There are several factors that make social engineering succeed, including the flaws of human nature and the commercial environment. This section briefly discusses these factors.

(a) Human nature

Berti and Rogers (2004:148) argue that being deceived has nothing to do with being less intelligent, but has everything to do with being human, and "being somewhat naïve, and having proper mind set and training to deal with" this kind of deception. Generally, people are trusting and co-operative by nature. This has been confirmed by studies in the field of social psychology that focused on human interactions (Dixit, 2013). These studies have found that almost everybody who is placed in the right circumstances and who interacts with a manipulative person can be influenced to behave in a particular way (Kalmbach, 2013). This may include revealing information he/she would not divulge under normal circumstances.

It has also been observed that people in authority exert a lot of influence over their subordinates (Jirasek, 2012). Depending on the morals and values of these people, their influence may be used in ways that constitute social engineering. According to Berti and Rogers (2004:148), in most instances, social engineering involves individual dynamics more than group dynamics. That is why most targets of social engineering are help desks and technical support staff and the interactions are mostly one-on-one, although not always face-to-face. The interaction may be online or virtual (Yoshikane, 2013; Kalmbach, 2013). People who use social engineering to commit computer crimes are always looking for prospective victims or rather individuals who appear to be susceptible to this kind of psychological attack.

(b) Commercial environment

Proff and Dettmann (2013) argue that the current commercial environment, which is characterised by rapid growth in ICT, creates a situation that is conducive for social engineering. ICT has led to the reduction of face-to-face interactions, but at the same time increased the rate of communication. Organisations are providing their employees with networked computers and thus their communication capacities have improved tremendously (Moore, Clayton & Anderson, 2009). ICT is used to communicate and do business with people who are unknown to each other physically. Due to human nature, people tend to trust and co-operate with counterparts they have not previously met.

The emphasis on team work and consumer satisfaction requires employees to be more civil and co-operative towards their colleagues, counterparts and customers (Moore et al., 2009; Proff & Dettmann, 2013). Whilst this is positive, it also lends itself to social engineering attacks. Customer service, friendliness and collaborative work make people in the business environment highly vulnerable to deception. Berti and Rogers (2004:148) report that it is difficult to measure the employees' sensitivity pertaining to information security when they perform their duties. This negligence and ignorance regarding information security has to change if companies want to deal with the risks, threats and crimes related to social engineering. Several authors assert that there are different motives for social engineering, including, but not limited to, intelligence gathering and political and business subversion (Williams & Karahanna, 2013).

(c) Intelligence gathering

Studies indicate that the main motive for social engineering is to obtain critical information (Singh & Singh, 2013). Studies have unfortunately also revealed that it is much simpler to collect sufficient sensitive information from a company and its employees in order to sound like an employee of that company (Dixit, 2013). Once the social engineer has gained sufficient information that enables him/her to sound and behave like a genuine employee of the company, he/she will then be able to penetrate its systems. Some conmen may steal the information that will enable them to talk and behave as if they belong to a certain regulator or law enforcement agency (Singh & Singh, 2013). Dagada and Mukwevho (2013) contend that attackers find it easier to examine the company information through its Website. Companies place a lot of information on their websites for marketing purposes. This information usually provides details such as staff lists, their contact details, branch offices and locations.

Whilst information published on a company's website is useful in attracting customers, it may also create a base for social engineering (Pozon, 2013; Dagada & Mukwevho, 2013). Most organisations have poorly constructed websites that are sources of easy intelligence-gathering. It is on these websites where companies give away critical information (Pozon, 2013; Singh & Singh, 2013). Goel and Shawky (2009) notes that, "going through an organisation's garbage can reveal invoices, correspondence, manuals etc." that would allow the attacker to collect critical information. Many convicted computer criminals have confessed to using the websites to gather critical information pertaining to their targets.

It has already been stated that the goal of intelligence gathering in the social engineering context is to enable the attacker to use the learnt information to sound and act as if he/she is a *bona fide* "employee, contractor, vendor, strategic partner, or, in some cases, a law enforcement official" (Berti & Rogers, 2004:149). The phenomenon wherein one acts like the legitimate person is called subversion (Pozon, 2013).

Launching social engineering attacks

Preparations for social engineering usually follow a gradual approach (Berti & Rogers, 2004). In most instances, social engineering attacks are similar to those of intelligence agencies when they infiltrate their targets (Chance-Hill & Odell, 2014). Social engineering attacks include target selection and the actual attack.

(a) Target selection

Once a sufficient amount of information has been collected from the targeted victim, the attacker will look for visible weaknesses in the organisation's staff (Berti & Rogers, 2004; Jirasek, 2012). Usually, help desk staff are the most common targets of social engineering. They are seen to be more willing to provide assistance, and they also deal with passwords and accounts. In most cases, the help desk staff is outsourced and thus they do not belong to the targeted company. This creates favourable conditions for successful attacks since the third party staff may not always know most of the targeted company's employees (Simonds & Christopher, 2013). Other than collecting information, another goal for social engineering is to gain a foothold in a targeted system. Attackers know that once they gain preliminary infiltration, it is easier to get more penetration, launch destructive attacks and erase their tracks.

After the help desk personnel, administrative assistants are the next most common targets of social engineering attackers (Newington & Metcalfe, 2014). Due to the nature of their job descriptions and work, administrative assistants are privy to huge quantities of information which usually move between members of senior management (Ioannidis, Pym & Williams, 2012; Dagada, 2013). However, social engineers prefer to know the names of the prominent people in organisations for the purpose of name-dropping. Sood and Enbody (2013) was surprised to realise that many administrative assistants know their managers' computer passwords. This is due to the fact that administrative assistants usually perform duties for their executives that require their executives' account privileges.

(b) Carrying out the actual social engineering attack

Social engineering attacks can be grouped into the following categories: firstly, attacks that appeal to the ego of the victim; secondly, attacks that take advantage of sympathy or empathy; and thirdly, attacks that are based on intimidation.

- Ego attacks

Social engineering attackers tend to appeal to the most primary human qualities – people like being told how intelligent they are (Warren & Leitch, 2010). Attackers use this human characteristic to get information from the employee of the targeted organisation. In most cases, this would be an employee who feels under-appreciated and that his/her position is beneath his/her skills. Usually, the victim does not know that he/she did something wrong (Williams, 2013; Ionnidis et al., 2012).

- Sympathy attacks

In this category, according to Berti and Rogers (2004:150), the social engineer usually portrays himself/herself, "to be a fellow employee (usually a new hire), a contractor, or a new employee of a vendor or strategic partner", who is experiencing difficulty related to the work and needs some help to perform a task urgently. The social engineer ensures that he/she wins the trust of the victims (McGraw, 2013). The attacker does this by name-dropping and appropriate jargon to win the confidence of the victim. The attacker may appear to be time-pressed to complete a task, but cannot because he/she has forgotten the account name or password, or has inadvertently been locked out.

The social engineering perpetrator tends to use the sense of urgency to win the sympathy or empathy of the victim (Berti & Rogers, 2004:150). However, the sense of urgency creates circumstances that are suitable for circumventing the necessary procedures. The attacker will then be able to get access in future without the assistance of the victim. Makinen (2013) and McGraw (2013) reasons that human beings naturally sympathise or empathise with the person who the social engineer is portraying himself/herself to be and thus in the majority of cases, victims innocently assist the attackers. If the attacker fails to get the required sympathy from the employee, she/he will keep on trying until such time one employee decides to assist (McGraw, 2013). Once the social engineer realises that the organisation is becoming aware of his/her attempts, he/she will withdraw.

- Intimidation attacks

In this category, according to Lu (2013), the social engineering attacker portrays him/herself as an authority figure. This can either be as a prominent person in the company or a law enforcement official. In this case, the attacker will target employees within an organisation who are on lower levels of the position he/she pretends to be occupying (Moore, Clayton & Anderson, 2009). The social engineer will create circumstances that will make it justifiable to ask for password information, account details, accessibility to the systems, or the required critical information (Navarra, 2013).

In a situation in which the social engineer pretends to be a law enforcement official, he/she may demand to access the systems or sensitive information that certain people have access to, such as, for example, national security concerns (Cox, 2012). Consequently, the employee may be instructed not to reveal the incident so that the investigation may not be hampered (Maswera, Edwards & Dawson, 2012). The attacker may even threaten the employee with a charge of defeating the ends of justice by divulging the incident. As with a sympathy attack, which has been dealt with above, the attacker will pretend to be in hurry, so that the necessary procedures are circumvented (Yaokumah, 2013). If the employee is not co-operating, he/she will be threatened with sanctions.

2.4.2 Breach of Privacy as an information security risk

This section demonstrates how ethical issues and privacy in particular can pose as information security risk. Privacy on the Internet; electronic database and privacy; traffic analysis and privacy; electronic surveillance and privacy; publicity attacks and privacy; and legal attacks and privacy are also discussed.

Privacy on the Internet

For several years, United States citizens have raised concerns about privacy after it came to their attention that information regarding their personal details was being stored in computer databases by government entities and commercial agencies (Saunders & Wu, 2011). As time went on, people in other parts of the world also started to express fears regarding the invasion of privacy. There is a growing awareness that using the Internet and the World Wide Web (WWW) affects that privacy (Hilmi, Pawanchik, Mustapha & Ali, 2013). In 2003, the USA-based advocacy group, Centre for Democracy and Technology, reported that only one third of USA government agencies inform visitors to their websites about the nature of information which is collected about them (Saunders & Wu, 2011; Overill, 2013).

Other studies reported that Internet users were sometimes reluctantly prepared to surrender their e-mail addresses online, but not other contact and personal details (Overill, 2013). Users tend to be very anxious concerning personal information, such as credit card numbers and identity numbers. The rapid availability and use of e-commerce in the corporate world allows companies to gather specific items of information. Some manufactures and companies put tracking numbers into their computer programmes and their Websites for information security purposes (Zissis & Lekkas, 2012).

Krause (2004) reports that in 1998, the United States Social Security Administration considered establishing a website that would allow full access to salaries and other personal details, which is contrary to the 1974 Privacy Act.

Electronic databases and privacy

Schneier (2000:33) observes that some technology has made it automatic for people to leave their "electronic footprints" on a regular basis. More of these "footprints" are being gathered and cross-correlated. Moreover, much of this kind of information is available on the Web (Roman, Zhou & Lopez, 2013). Due to the electronic databases, it is easy to compile a dossier about a particular person.

Most electronic databases are for commercial purposes and include major credit databases, such as those owned by Equifax, Experian, and TransUnion (Roman et al., 2013). There are also large electronic databases containing records of telephone calls, credit cards, individual purchases, individual health status and other personal details. These electronic commercial databases can be used by their owners, creators or be sold for other purposes. The web has thus exacerbated privacy violations. Some online retailers store records of products and services which individual consumers buy. According to Schneier (2000:33), the online stores "can also keep records of everything you look at, every item you ask to see more information about, every topic you search for, how long you spend looking at each item – not just what you buy, but what you look at and don't buy". Google has the same feature and may predict what you are looking for (Hilmi et al, 2013).

Simmonds and Christopher (2013) reported that these electronic databases are very useful in law enforcement. The police use them to fight crime by downloading a criminal record automatically. Whilst this should be applauded, it could also lead to privacy invasion (Kshetri, 2013). Hackers can break into the very police database and steal some individual's personal information for whatever purposes. Schneier (2000) and Kshetri (2013) reasoned that police databases are not necessarily better secured than corporate databases while the information they contain is even more sensitive.

Traffic analysis and privacy

According to Schneier (2000:34) traffic analysis involves the study of communication patterns – not the content of the message – but characteristics about them: "Who communicates with whom? When? How long are the messages? How quickly are the replies sent, and how long are they? What kinds of communication happen after a certain message is received?" These are typical traffic analysis questions and their answers can disclose a lot of personal information. Lu (2013) were quick to warn that traffic patterns of communication are as crucial as the content thereof. Schneier (2000:34) provides an example to support the above assertion: "The simple fact that Alice telephones a known terrorist every week is more important than details of their conversation. The Nazis used the traffic analysis data in itemised French phone bills to arrest friends of the arrested; they didn't really care what conversations were about".

Some authors observe that even if one encrypts his/her web traffic, traffic analysis drawn on the amount of the encrypted web pages is an adequate picture to indicate what one is browsing (Thompson, 2014). Scheneier (2000) and Burda and Teutenberg (2013) argue that although militaries have used traffic analysis for many years, it remains a relatively new area of research in academia.

Electronic surveillance and privacy

Interception of e-mail communication by intelligence agencies around the world could be interpreted as a violation of the public's privacy (Burda & Teutenberg, 2013). In some cases, this kind of interception or electronic surveillance is illegal even though it is carried out by government law enforcement agencies. Schneier (2000) as well as Mamaghan, Madani and Sharifi (2012), report that several intelligence agencies used an automated interception system to intercept about 3 billion communications daily. These include e-mail messages and Internet downloads (Mitropoulos, Othonos & Douligeris, 2013).

Intelligence agencies reported to be using this automated interception system include the United States, the United Kingdom, Canada, Australia and New Zealand. The system collects communications indiscriminately, "then sorts and distils the information through artificial intelligence programmes" (Schneier, 2000:35). This statement is supported by Burda and Teutenberg (2013).

Publicity attacks and privacy

There are hackers who launch attacks on a critical system like government communication networks and the military in order to gain publicity. Most publicity seeking system attacks are launched by skilled hackers who are very familiar with systems and their security (Gupta, Jin, Sanders, Sherman & Simha, 2012). They usually have access to resources that enable them to break the system.

By breaking into the system, the victim's privacy becomes vulnerable to the hacker and possibly the media (Nehinbe, 2012). On the other hand, the very fact that the media will publicise a successful hacking can, in some cases, constitute a privacy violation of the company being victimised. It should, however, be borne in mind that publicity seeker system attackers do not belong in the same threat category with criminals. According to Schneier (2000) and Mamaghan et al. (2012), criminals only launch an attack if they will benefit materially; publicity seekers will attack a system if there is a possibility of the media covering it. Large scale systems that are owned by prominent organisations are more likely to be victims of the publicity seeker hackers.

Schneier (2000) argues that in some instances, the rationale for these attacks is the desire to correct the problem. Most organisations appear to ignore their information security weaknesses until they are revealed publicly. Once a certain newspaper announces the attack, the victim organisation will rush to correct the problem. In this way, the publicity seeking attackers have increased the security of the victim's systems (Demirkan & Delen, 2013; Mitropoulos et al, 2013).

The problem with the publicity seeking attacks is that it damages the integrity and reputation of the company attacked (Stone, 2013). The victim company will soon realise that the negative publicity is very costly (Schneier, 2000; Nehinbe, 2012). Customers and investors will naturally shy away from a company whose information security is vulnerable (Singh & Singh, 2013).

Legal attacks and privacy

There are social activists or customers who will reveal the vulnerability of a weak security system by challenging it through the judicial system. According to Schneier (2000:40): "The aim here isn't to exploit a flaw in a system. It isn't even to find a flaw in the system. The aim here is to persuade a judge and jury (who probably aren't technically savvy) that there could be a flaw in the system". This can be achieved by discrediting the system, to put sufficient doubt in the minds of the judge and the jury that the system has some security loopholes (Andoh-Baidoo, Osei-Bryson & Amoako-Gyampah, 2012).

There are occasions when organisations will take a suspected criminal to court, only to be proven wrong. Schneier (2000:40) reports that in 1994, in the United Kingdom, a certain client found his bank account emptied, and, "When he complained about six withdrawals he did not make, he was arrested and charged with attempted fraud. The British bank claimed that the security in the ATM system was infallible, and that the defendant unequivocally guilty. When the defence attorney examined the evidence, he found, (1) that the bank had no information management or quality assurance for its software, (2) that there was never any external information security assessment, and (3) that the disputed withdrawals were never investigated. In fact, the bank's programmers claimed that since the code was written in assembly language, it could not possibly be the problem (because if there was a bug, it would cause the system to crash). The man was convicted anyway. On appeal, the bank provided the court with a huge information security assessment by an auditing firm. When the defence demanded equal access to their systems in order to evaluate the information security directly, the bank refused and the conviction was overturned." This assertion is also supported by authors such as Williams and Karahanna (2013) and Andoh-Baidoo et al., 2012).

It is clear from the above information that a number of the aforesaid bank's information security issues were made public during the court case and jeopardised its privacy regarding information security and internal operational policies. The legal system attack is very forceful. Isaacs (2013) observed that people who resort to legal attacks are very skilled in dealing with high profile cases. Furthermore, they are able to access many resources, including researchers and technical experts. Schneier (2000:41) concludes that a legal attack should be viewed, "as a publicity attack with a bankroll and more relaxed victory conditions". This point of view is supported by authors such as Navarra (2013) and Isaacs (2013).

2.4.3 Copyright as a information security risk

The inception of ICT and the Internet in particular has led to the abundance of information available in many forms. Networked computers globally and the Web provide a platform for access to ever increasing amounts of information (Silva & Fulk, 2012), yet the same technological platforms that enable access to information create copyright and intellectual property rights challenges (Rahman & Ramos, 2013).

Internet and benefits of copying, using and distributing online materials

The Internet has provided many opportunities for sharing information, art, music and other works internationally (Ting & Yi, 2013) but, whilst the Internet has opened up a wide range of benefits to its users, there are serious concerns amongst copyright owners about maintaining control over the copying, using and distribution of their work (Silva & Fulk, 2012). This should be attributed to the ethical issues emanating from copyright in the Internet arena (Jairak & Praneetpolgrang, 2013). It should also be emphasised that copyright in the computing environment lends itself to information security problems, challenges and crimes. The information security concerns arise because the nature of the online environment makes it easier for some people to copy and/or distribute literature and audio-visual items than in the physical word (Strang, 2013).

Copyright challenges are aggravated by the simplicity of producing multiple copies of online materials quickly (Pardo, Pino, Garcia, Baldassarre & Piattini, 2013). On the other hand, these online materials are internationally available and Internet users are able to hide their identities. Given the information security problems posed by the copying, using and distribution of online-based materials, it is anticipated that copyright owners will increasingly turn to other measures to assist them with enforcement of their rights (Julisch, 2013; Jairak & Praneetpolgrang, 2013).

Internet challenges the status quo of property rights and intellectual property protection

According to Tsolis, Tsolis, Karatzas and Papatheodorou (2002:53), “the evolution of technology is challenging the status quo of intellectual property protection” and the management thereof, in various ways. The situation is exacerbated by the fact that users of the copyright information in whichever form ─ print, digital, material, music, films – have some expectations about their own right to, “use and copy that information and to communicate it to others” (Kauffman, Techata & Wang, 2012: 117). This is highly problematic because although users rightly have expectations, they do not necessarily have the legal right to conduct the aforesaid activities without the permission of the copyright owner (Paliwala, 2013). Notwithstanding this, users have, for many years, acted on their expectations without ramifications.

2.4.4 Measures to deal with ethical issues

As explained, for the purpose of this study, ethical issues are constituted by social engineering, privacy, and copyright (see section 2.4). This section provides an overview of defence mechanisms against ethical related issues within the context of the ICT domain. Although social engineering, privacy, and copyright are different ethical concepts, their defensive measures are similar, and include physical security, administrative measure, policy and legal education.

Physical security measures

According to Koskosas (2012), ICT ethical related risks, threats and crimes can, amongst other things, be dealt with by providing adequate physical security. This is supported by Cox (2012) and Pardo et al. (2013), who suggests that physical security is the easiest to comprehend and possibly the simplest to implement. Berti and Rogers (2004:147) describes physical defence of the security of tangible and intangible assets from, “theft, vandalism, catastrophes, natural disasters, deliberate or accidental damage, and unstable environmental conditions such as electrical, temperature, humidity, and other such related problems.”

Efficient physical security requires adequate building and facility construction. This view is supported by Berti and Rogers (2004:147) who argue that building and facilities that house ICT infrastructure require, “emergency preparedness, reliable electrical power supplies, reliable and adequate climate control, and effective protection from both internal and external intruders.”

Logical and administrative security measures

Logical and administrative security can be employed to protect information assets. According to Alazab and Venkatraman (2013), logical security uses technical solutions to protect information assets. Berti and Rogers (2004:152) provides the following examples of technical measures: "firewall systems, access control systems, password systems, and intrusion detection systems." Schneider (2000:30), however, cautions that technical controls can be productive but they also depend on the human element to be effective. Administrative security, on the other hand, is those measures that usually include policies and procedures (Schneider, 2000; Koskosas, 2012). Although these measures do not employ controls, they deal with ICT ethical related risks, threats and crime.

Policies, awareness, and education

ICT ethical related risks, threats and crimes are difficult to counter. This is attributed to the fact that technical security controls are not always effective as protection mechanisms (Schneider, 2000; Xiong, 2013). Ethical problems, such as social engineering, for example, are attacks targeting the human element (Makinen, 2013). It is on this basis that protective measures need to focus on user centred information security defences. These measures are constituted by policies, users' awareness and education. Schneider (2000) strongly suggests that policies should be introduced and publicised to the whole enterprise as a measure to counter ethical related problems. Policies are very useful in providing guidelines on how people should behave (Gupta & Narain, 2012).

2.5 INFORMATION SECURITY POLICIES

Information security policies play a critical role when dealing with information security risks (see §1.2.3, §2.4.4, and Chapter 6 of this thesis). In actual fact, the main aim of this study was to investigate how corporate South Africa employs policy and legal aspects in their endeavours to provide information security. Most information security-related policies in the corporate environment are in fact derived from relevant sections of legislation. Maiwald (2004:144) observes that policy formulation is a "thankless job" since most people within organisations do not like being regulated: "Policy sets rules. Policy forces people to do things they do not want". The aforesaid assertion is still relevant at the present time (Gonvalves & Jesus, 2013).

This section reflects on the necessity of information security policies and the policy management hierarchy. The findings of this study related to information security policies are found in Chapter 6.

2.5.1 The rationale for information security policies

Policies are essential in the provision of information security as they provide rules that guide the configuration of the systems and actions of users within an organisation (Rogerson & Milton, 2013). Policies explain how information security should be implemented and maintained. Policies define the appropriate measures to employ when protecting information assets and systems (Gonvalves & Jesus, 2013). According to Goo and Yim (2014), information security policies are not merely confined to technical mechanisms but they also define how employees should behave when they are using information systems that belong to or are connected to the organisation's network. Nichols-Hess and LaPorte-Fiori (2015) declares that policies define how organisations should operate information systems under both normal and unusual circumstances. If a security breach or systems failure occurs, the organisation policies and procedures should provide guidelines on correctional and remedial steps to be taken.

Another reason for employing policies in the provision of information security is that they tend to put everybody within a company on the same footing (Maiwald, 2004). For that reason, each person in an organisation should work within the operational framework that has been provided by the policies and procedures. This will assist in the provision of information security. Goo and Yim (2014) supports this view and claims that policies provide the scope for the employees in the same organisation to work together in ensuring that information and systems are protected. On the other hand, Mainwald (2004:144) has observed that policies and procedures define the goals and objectives of the organisation's information security programme. If these goals and objectives are well communicated to all employees, the basis for organisation wide security teamwork will be established. This observation is supported by (Nichols-Hess & LaPorte-Fiori, 2015)

Interestingly, Schneier (2000:308) compared information security policies with the government policy on foreign affairs: "When a government is accused of not having a coherent foreign policy, it's because there is no consistency in its actions: no overall strategy. Similarly, a digital system without security policies, is likely to have a hodgepodge of countermeasures". This view is supported by Niu and Reith (2014). In the provision of information security, the policy is glue that put everything together (Nichols-Hess & LaPorte-Fiori, 2015).

According to Schneier (2000:308), the policy is about the information security strategy: "You can't decide what kinds of antifraud countermeasures you need for your cell phone unless you have a policy you want those countermeasures to enforce." Equally, one cannot expect several information officers who are responsible for the system security to carry-out their functions coherently in the absence of policies that guide their actions and they are supposed to follow.

2.5.2 The policy management hierarchy

These following paragraphs will demonstrate that there are three main categories of information security policy: regulatory, advisory and informative.

Regulatory policy

Hare (2004) declared that it is imperative for each organisation to have an information security policy that results from legislation. In South Africa, the King III Report (2009) directs the Board of Directors to establish information security-related policies. Although the King III Report is not legislated, organisations listing on the Johannesburg Stock Exchange (JSE) are compelled by law to adhere to its provisions (see Paragraph 1.2.5 of this thesis). It is on this basis that South African organisations should establish information security policies as a response to the regulatory requirement. Inevitably, some of these policies will have to address information security in the e-Commerce environment. On the other hand, information security policies should have a section referring to the South African laws it is based on. These include the Electronic Communications and Transactions Act No. 25 of 2005, the Promotion of Access to Information Act No. 2 of 2000, the Regulation of Interception of Communications and Provision of Communication-related Act No. 70 of 2002, and the Protection of Personal Information Act No. 4 of 2013.

Other than complying with the regulations, information security regulatory-aligned policies should provide consistent operational and behavioural processes (Niu & Reith, 2014). Organisations that provide services and/or products to the consumers are expected to show some similarities regarding the application of the regulations without prejudice.

Advisory policies

Goncalves and Jesus (2013) reports that advisory policies are targeted at knowledge for employees to enable them to make informed decisions regarding information security-related situations. The enforcement of the advisory policy is usually not applied with much effort. Nevertheless, the policy will mention the implications for not applying the advice provided in the policy (Goo & Yim, 2014). According to Hare (2004:934), the possible impact associated with non-compliance includes, but are not limited to, the following:

- Omission of information that is required to make an informed decision.
- Failure to notify the correct people who are involved in making the decision or to complete the process.
- Missing important deadlines.
- Lost time in evaluating and discussing the alternatives with auditors and management.

The above points remain relevant (Nichols-Hess & LaPorte-Fiori, 2015). Goncalves and Jesus (2013) emphasises the fact that failure to comply with the information security advisory policy can be substantial to the organisation. The aforesaid claim is supported by Hare (2004:934), who notes that the cost of squandered productive time attributable to the consideration of alternatives can have a strong impact on the organisation.

Informative policy

The purpose of the informative policy, according to Hare (2004) and Niu and Reith (2014), is to communicate certain information security issues to a particular audience. There are no penalties for not complying with this kind of policy. Whilst the informative policy is lesser in stature when compared with both regulatory and advisory policies, it conveys important information security-related messages to the targeted audience (Rogerson & Milton, 2013). The next section presents a summary of this chapter.

2.6 SUMMARY

This chapter has provided broad insights on information security history, risks. Chapter 1 explained the overall purpose of this study, which is to assess how organisations can, amongst other things, use legal aspects to address their information security concerns. The legal and policy aspects pertaining to information security do not occur in a vacuum and thus a broader understanding of issues that constitute information security risks is essential. Therefore, this chapter examined and defined information security risks such as hacking, viruses, privacy, ethical issues and social engineering. The chapter reviewed the history of information security because for organizations and individuals to be successful in attempting to secure existing systems and networks, there is a need to draw on the comprehensive pool of information security that exists. It is important to understand how information security crimes were committed and what measures were put in place to prevent more sophisticated crimes from taking place. This chapter also presented a brief overrview of the information security policies. The next chapter presents the South African legal framework with regards to information security.

CHAPTER THREE
THE SOUTH AFRICAN LEGAL FRAMEWORK REGARDING INFORMATION SECURITY

3.1 INTRODUCTION

As mentioned in preceding chapters, dealing with information security problems requires the application of relevant policies. These policies should be based on international and national frameworks. Whilst the previous chapter focused on information security issues, this chapter will deal with the legal framework in South Africa and how it relates to information security.

There are several laws in South Africa which deal directly or indirectly with information security issues. These laws relate to, amongst others, trademarks, malicious code, hacking, copyright, patents and privacy, to name but some of the issues. It is thus important that South African companies base their information security policies on these laws. These laws include, but are not limited to, the following: the Constitution of the Republic of South Africa (1996); the Promotion of Access to Information Act No. 2 of 2000; the Companies Act No. 71 of 2008; the Electronic Communications and Transactions (ECT) Act of 2002; the National Credit Act No. 34 of 2005; the Protection of Personal Information (PoPI) Bill of 2007; the Copyright Act of 1978; the Labour Relations Act No. 66 of 1995; the Regulation of Interception of Communications and Provisions Communication-related Information (RICA) Act No. 70 of 2002; Consumer Protection Act No. 68 of 2008; and the King III Report. This list is not exhaustive, but includes the most significant legislation that governs information security in South Africa.

It is useful to clarify, for the purposes of this research, the difference between a bill and an act. The Bill is a draft law submitted to Parliament by the relevant Minister (Member of the National Executive) for consideration. Once Parliament passes the Bill and the President signs it, it becomes an Act (law). The chapter also reviews the King III Report. This is not, however, a law, but a set of recommendations with which all companies listed on the

Johannesburg Stock Exchange are legally compelled to comply. It was therefore deemed necessary to include it in this chapter.

3.2 THE PROVISIONS OF INFORMATION SECURITY ISSUES IN THE CONSTITUTION

The Constitution of the Republic of South Africa (1996) is the supreme law of the Republic and is the foundation of all laws passed by the South African Parliament. The Constitution has a direct impact on information security related issues, in particular, the Bill of Rights. Taken at face value, one may deduce that the constitutional provisions related to information security contradict each other. Such provisions include the following: privacy vis-à-vis access to information; and freedom of expression vis-à-vis human dignity. The legislators were aware of these rudimentary contradictions and thus Clause 36 of the Constitution prescribes limitations of rights. No right should be exercised at the expense of other rights. In other words, the right to freedom of expression cannot be exercised in a manner that undermines someone’s human dignity.

The following are some of the South African government laws that address IT-related risks, threats and cyber-crime:

- Protection of Personal Information (PoPI) Bill of 2009;
- Privacy and Data Protection Act of 2006;
- Electronic Communications and Transactions Act of 2002 (ECT Act, 2002);
- Regulation of Interception of Communications and Provision of Communication-related Information Act of 2002 (RICA Act 2002);
- Promotion of Access to Information Act No. 2 of 2000;
- Patents Act No. 57 of 1978;
- Copyright Act No. 98 of 1978;
- Intellectual Property Laws Amendment Act No. 38 of1997; and
- Trade Marks Act No. 194 of 1993.

3.3 COPYRIGHT LAW IN THE INFORMATION SECURITY CONTEXT

The inception of ICT and the Internet in particular has led to the abundance of information available in many forms. Computers networked globally and the World Wide Web (WWW) provides a platform for access to ever increasing amounts of information (Schonwetter, Ncube & Chetty, 2010). Yet the same technological platforms that enable access to information create copyright and intellectual property rights challenges (Lu, 2013).

3.3.1 Internet and benefits of copying, using and distributing online materials

The Internet has provided many opportunities for sharing information, art, music and other works globally (Lee, 2012). Yet, whilst the Internet has opened up a wide range of benefits to its users, there are serious concerns amongst those who have copyright to sustain control over the copying, using and distribution of their material. This relates to the ethical issues emanating from copyright in the Internet arena (Lee, 2012; Wu & Sun, 2013). It should also be emphasised that copyright in the computing environment lends itself to information security problems, challenges and crimes. The information security concerns arise because the nature of the online environment makes it possible for literature and audio-visual items to be copied and/or distributed other than in the physical world without affecting the original.

These copyright challenges are aggravated by the simplicity of producing multiple copies of online materials quickly (Paterson, 2012). In addition, these online materials are internationally available while Internet users are able to hide their identity. Given the information security problems posed by the copying, using and distribution of online-based materials, it is anticipated that copyright owners will turn to other measures to assist them with the enforcement of their rights.

3.3.2 Internet challenges the status quo of intellectual property protection

According to Tsolis et al. (2002:53), “the evolution of technology is challenging the status quo of intellectual property protection” and the management thereof in various ways. The situation is exacerbated by the fact that users of the copyright information in whichever form, whether print, digital, material, music or films, have some expectations about their own right to “use and copy that information and to communicate it to others”. This is problematic because, although users rightly have expectations, they do not necessarily have a legal right to undertake such activities without the permission of the copyright owner (Washah, 2013), although in fact users have for many years acted on their expectations without consequences (Paterson, 2012).

3.3.3 Infringements of copyright and legal remedies in South Africa

Herman (2012) suggests that there are several measures to deal with copyright crime, including physical security and logical and administrative security measures. Herman (2012) further emphasises user education and the use of policies as effective measures to deal with infringements of copyright. It is critical to bear in mind that policies should be informed by the relevant legislation.

South Africa is informed by the Copyright Act No. 98 of 1978. Although this Act is not recent, it is still effective in South Africa and it has been augmented by regulations published in 1985. According to Clause 23 of the Copyright Act, the infringement of copyright is constituted by, among other things:

(i) The encroachment of copyrights by any other person, other than the owner, who uses the rights without permission from the owner. Examples of such encroachment would include:-

  a) Bringing items into the country to be used differently from the intended owner’s use. The abuse here could be in terms of selling, letting or hiring the item in the country

  b) Unlawful acquisition of software in the country

(ii) The encroachment of copyrights could also be committed when a person who gives permission to another to use places of public entertainment where the individuals use items like music without proper permission from the copyright owner.

The next section deals with penalties for infringement.

3.3.4 Action by owner of copyright, and penalties for infringement

Regarding the action which copyright owners can take when their rights have been infringed, Clause 24 of the Copyright Act No. 98 of 1978 stipulates that:

(i) Use the same margins as above for (i) and (ii) or change the above to be the same as this Any item produced due to infringement of copyright should be made available to the plaintiff. In case of damages, the plaintiff will be paid the amount which the licensee would have paid for the activity concerned. However, according to the clause, the copyright owner may in writing, before establishing the course of action, inform the licensee about the proceedings. The licensee may intervene and pay for the damages incurred.

(ii) In the case where the offender did not know about violating any copyrights, damages may not be paid for the infringement. However, in the case where the infringement is admitted or liability is otherwise proven then the offender will be required to pay for all damages relating to the violation as assessed by the court.

Regarding the penalties incurred as a result of infringement, Clause 27 of the Copyright Act No. 98 of 1978 stipulates that:

(i) If the individual is convicted for the first time, then he or she will get a fine of not more than five thousand Rand or imprisonment for not more than three years. However, the offender may be subjected to both paying the fine and the imprisonment for the individual articles related to the infringement.

(ii) If not the first offence, then the offender could get a fine of not more than ten thousand Rand or imprisonment for not more than five years. The offender may also be subjected to both paying such a fine and imprisonment for the individual items related to the infringement.

3.3.5 Reproduction regulations and permitted reproduction

The Copyright Act No. 98 of 1978 with Regulations of 1985, regarding reproduction of a piece of work, stipulates that reproduction of a work is permitted provided only one copy of the piece of work is reproduced. Again, reproduction may be permitted if the repeated copies are within the acceptable exploitation of the production and author's rights. With these regulations in mind, libraries or archives may reproduce a work with its employees acting solely within the scope of their job. According to the Copyright Act No. 98 of 1978 Regulations of 1985, the employees may distribute the reproduction on the condition that:

(i) there is no intention of establishing by deduction direct or indirect commercial advantage;
(ii) the recreated work shall be open to the public or available to researchers affiliated to the library or archive depot;
(iii) the recreated work incorporates a copyright warning;
(iv) reproduction rights and distribution conform to a copy of an unpublished work duplicated in facsimile form completely for purposes of preservation and security;
(v) the library or archive depot shall display prominently, at the place where orders are accepted, and include on its order form, a copyright warning.

The section below provides an example of copyright case law.

3.3.6 Judgement regarding infringement of copyright in South Africa: Sure Travel v Exel Travel

A High Court judgment made on the 19th November 2004 regarding the infringement of copyright between Sure Travel and Exel Travel has had an effect on the interpretation of copyright law in South Africa (Buys, 2006). This judgement assessed the extent of software protection and how to prove the infringement thereof.

About the case and its judgement

Sure Travel, the company which has a travel agent's franchise, makes use of a new software application known as Matchmaker. The respondents in the case, as a franchised agent of Sure Travel, signed a contract that included their right to use the Matchmaker system. Later the respondents abandoned Sure Travel group to establish their own group of travel agents. However, they continued using the software application. Consequently, Sure Travel alleged that the continued use of the software application violated the rights attached to the

Matchmaker system. Since the respondents broke the contract with Sure Travel, they were hence unlicensed to continue using the software application.

According to Buys (2006), Sure Travel's application for an interdict was dismissed by the court on the basis that Sure Travel, the complainant, failed to prove that the Matchmaker system contained any confidential or proprietary information. Again, based on this argument, the court also ruled that no unlawful competition took place. The section below deals with e-commerce.

3.4 E-COMMERCE PATENTS LAW IN THE INFORMATION SECURITY CONTEXT

3.4.1 Overview of patent law

Patents are the basic protection provided for inventions. According to Bagby (2003:233), patents are a strong form of Intellectual Property and thus "patent law protects inventions". The invention process includes the production or machination of a product not known before. This may be as a consequence of creativity or research. According to Bagby (2003:233), a patent is a limited monopoly licensed by the government to the initial producer of "useful, novel, and non-obvious inventions." Patents for inventions are not easily distinguishable from trade secrets. The fact is that the patent system grants the inventor of new and innovative technology limited right to prevent others from practising the technology, as an encouragement and in exchange for releasing the technology to the public. The patent laws have contributed immensely to the success of US technology during the past two centuries (Wu & Sun, 2013).

It was imperative for patent law to be applicable to e-commerce in particular. In effect, the patent system has proved to be valuable for ICT and thus Berman, Reister and Kregel (2003:6.1) reported: "As with many new technologies, there has been a "land grab" rush to obtain Internet technology and Internet business method patents, and some relatively broad patents have been issued." This assertion is supported by, *inter alia,* Xu and Sun (2013).

3.4.2 Types of e-commerce patents

An e-commerce patent is defined as a patent that can be granted to an organisation/individual conducting business through the Internet (Yaokumah, 2013). Liu (2013) went further to observe that patents can cover technology that (1) provides a better or different experience for a Website's users (user experience patents); or (2) makes the e-commerce more efficient or more profitable (business enhancement patents). In addition, several broad aspects involve technology that is basic to the Internet operation (common use patents) (Yoshikane, 2013).

Berman et al. (2003:6.02) provides examples of types or groups of patents to demonstrate several aspects of patent law pertaining to e-commerce:

- Amazon's one-click patent, which covers methods for enabling consumers to buy items on the Internet with a single click (a user experience patent);
- Priceline's reverse-action patents, which cover methods for enabling consumers to name their own prices for goods or services (user experience patents);
- Patents held by numerous different companies on targeted advertising, which cover ways of directing particular advertisements to users based on information about those users (business enhancement patents); and
- e-Data Corporations Freeny patent, which its owner originally asserted covered all Internet sales involving downloads of digitised material, such as music (a common use patent).

The views of Berman et al. (2003) are supported by several authors, including Collan, Fedrizzi and Luukka (2013) and Issacs (2013). In most countries, patent rights are enforced through civil litigation in a court designated for this purpose in a particular country.

3.4.3 Provisions of the South African Patents Act

The legislation that specifically focuses on patents in relation to Information in South Africa includes the Intellectual Property Laws Amendment Act No. 38 of 1997, and the Patents Act No. 57 of 1978. The Intellectual Property Laws Amendment Act No. 38 of 1997 is constituted by sections of various Acts in South Africa:

- Sections 1-18: Amendment of Merchandise Marks Act No. 17 of 1941;
- Sections 19-25: Amendment of Performers' Protection Act No. 11 of 1967;
- Sections 26-49: Amendment of Patents Act No. 57 of 1978;
- Sections 50-58: Amendment of Copyright Act No. 98 of 1978;
- Sections 59-68: Amendment of Trade Marks Act No. 194 of 1993;
- Sections 69-79: Amendment of Designs Act No. 195 of 1993; and
- Section 80: Short title and commencement.

For the purposes of this study, the main focus will be on the Patents Act No. 57 of 1978, hereafter referred to as the Patents Act. The provisions reflected in the paragraphs below are those that have an impact on information security.

Patentable inventions

In accordance with clause 25 of the Patents Act, patents are granted for new inventions with the capacity to benefit industries. However, a patent is not granted for any invention that may encourage immoral or offensive behaviour. The patent is also not available for a new invention for production of living things that are not subjected to micro-biological processes.

Debate about the legality of software patents in South Africa

According to the article written by ICT journalist, Brian Bakker (2007:26), software patents are supposedly not legal in South Africa. They should not be deemed legal until such time as they are proven to be by the legislator of the Court of Law. Section 25 (reflected above) of the Patents Act indicates that software (a programme for a computer) cannot be registered as a patent in South Africa. According to Bakker's (2007) article, "this prohibition takes the form of an explicit exclusion, one of seven". He quotes the Innovation Fund's Biago: "The Act basically says that computer programmes 'as such' shall not be an invention. Everybody asks how the 'as such' is supposed to be interpreted but, unfortunately, we don't yet have any case law in South Africa regarding the patentability of computer programmes". The CSIR's Bob Joliffe who is also mentioned in the aforesaid article argued that there is a huge amount of case law in Europe which may inform the South African judgements if and when they happen. Joliffe claimed that the South African patent law "was essentially copied from the UK statute which, in turn, was derived from the European Patent Convention. As a result, the language is almost identical." This situation remains unchanged to date (Behr, 2013; Collan et al., 2013), and will be dealt with in detail in the findings of this study.

Disputes as to the rights in or to patents

As stated in Section 28 of the Patents Act, rights disputes between individuals should be settled by the commissioner following an application by any of the parties. If, however, an individual is not willing or is not able to participate in an application for a patent, the individual may be asked to execute an assignment by the commissioner. If the execution is just and equitable according to the commissioner, the compensation may be due to the non-participating individual.

In a situation where an individual declares a right to exclude any other individual from applying for a patent, directions from the commissioner may require such other individual to perform any deed of assignment that may be requested and that the deed of assignment be extended to other countries.

Infringement of the patents

In conformity with Section 65 of the Patents Act, which provides the proceedings for infringement, the patentee may file such proceedings regarding a patent. The complainant may be compensated through an interdict, or by bringing to him/her the infringed products, or the damages. However, the accused may react for annulment of the copyright based on any base on which such a copyright may be revoked. Nevertheless, before filing such proceedings, the complainant should provide a notice to the registered licensee of the copyright in question, who may have the right to intervene as a co-complainant. In the case of damages, the complainant may opt for an amount which the defendant could have paid in respect of the copyright in question, as compensation. The section below deals with trademarks legislation.

3.5 TRADEMARKS LEGISLATION IN THE INFORMATION SECURITY CONTEXT

3.5.1 Overview of the Trademark concept

This section provides an overview of the trademark law in the context of e-commerce and information security in particular. Before one focuses on the trademark law, it is important to understand the meaning of the word *trademark*. A trademark, according to authors such as Leverich, Gallagher-Duff, Lavelleye and Rosette (2003:7.01), "is a distinctive work, name, phrase, symbol and/or design that identifies and distinguishes one's goods (or services) from the goods and services of others." Bagby (2003) opines that trademarks are the most significant form of recent commercial symbols. Trademarks are the compartment of business-related symbols that obtain legal protection. This view is supported by authors such as Proff and Dettmann (2013) and Simon (2013).

Trademarks law grants the owner of the trademark the right to prevent other individuals or/and entities from employing the trademark or *mark* to market their products or services (Proff & Dettmann, 2013). According to Bagby (2003:278), trademark law is a complicated and challenging field, "because the standards of analysis and much of the case law are based on artistic and cognitive judgements about human perception and commercial behaviour." This assertion is supported by authors such as Behr (2013), Assaf (2012). This section will mainly focus on the South African Trademarks Act No. 194 of 1993 and how it pertains to information security.

3.5.2 South African trademark law

Trademarks - Registration and Penalties

In accordance with Section 16 of the Trademarks Act No. 194 of 1993 regarding an application for registration, it is required that such application should be made to the registrar as recommended. Based on the Act, the registrar may accept the application or conditionally accept it, or reject it provisionally or completely reject. In the situation of conditional acceptance and provisional rejection, the registrar should, in writing, advise the reasons for the decision made. However, at any point in time, the court or registrar may make corrections to mistakes in, or in connection with, the application or ask the applicant to make any recommended amendments as deemed fit.

Section 11 of the Act outlines a framework to be followed when registering trademarks regarding particular services or goods. According to this section, registration of a trademark for such services or goods should be made in accordance with the dictated classification as deemed fit on the registration date.

Punishment regarding registration fraud is stipulated in Section 60 of the Trademarks Act No. 194 of 1993. According to this section, any individual who provides or influences untrue information regarding the registration commits an offence and should be subjected to paying a fine or face imprisonment for not more than a year. If any individual uses a mark which is not registered as a registered trademark, according to Section 62 of the Act, s/he commits an offence and should be fined or imprisoned for not more than 12 months.

3.5.3 A trademark judgement in South Africa: Nandos v Farkhi

The World Intellectual Property Organisation's (WIPO) Arbitration which took place in South Africa on 23 May 2000 with Justice Austin Amissah presiding, has influence on the interpretation of trademark law in South Africa (Buys, 2006). The subsections below provide some detail regarding the case.

About the case and the judgement

"Nandos" and "Nandos Chickenland" were trademarks registered and used both locally and abroad for trading by the plaintiff continuously from 1989. Despite the effort to own the rights of the domain names <nandos.com> and <nandoschicken.com>, the plaintiff was unsuccessful because of the earlier registration by some other party. VWV Interactive, previously the plaintiff's Internet Service Provider, tried to obtain the <nandos.com> domain name in May 1998. However, they could not succeed due to the payment the registrants demanded, which, according to the plaintiff, was excessive. In 1999, the plaintiff tried again to gain the domain name after switching on to Digital Mall as its Internet Service Provider. It was during this process that the plaintiff discovered that the defendant had already registered <nandoschicken.com> as a domain name and that they had legal control of the domain name

<nandos.com>. However, the domain names in question were, as yet, not attached to any website.

According to the judging panel, the plaintiff's registered trademarks and the domain names registered by the defendant were perplexingly similar, and therefore ruled that the registration of the domain names by the defendant was *mala fide* and the defendant thus had no rights to the domain names. The panel accepted the plaintiff's request to take over the possession of the domain names <nandoschicken.com> and <nandos.com>.
The next section reflects on the patents laws.

3.6 PRIVACY LAWS IN THE INFORMATION SECURITY CONTEXT

The violation of privacy electronically is considered to be an information security problem. The Bill of Rights in the Constitution of South Africa (2006) stipulates the right to privacy – **everyone has the right to privacy**, which includes the right not to have:

- their person or home searched;
- their property searched;
- their possessions seized; or
- the privacy of their communications infringed.

There are various laws in South Africa which protect privacy and provide for privacy based on the abovementioned constitutional directives.

3.6.1 Protection of personal information

The PoPI Bill No. 9 of 2009 specifies in Clause 11 that, "personal information **must** be collected for a specific, explicitly defined and legitimate purpose." Furthermore, the person whose information is gathered should be made aware of the purpose of collection and the recipients of such personal information. As stated in Chapter 1 of this thesis, on 27 November 2013 the President of South Africa signed the aforesaid Bill into law as the PoPI Act No. 4 of 2013. This study focused on the Bill since the Act was only signed into law when this study was being finalised.

The Electronic Communications and Transactions Act No. 2 of 2002 (ECT Act 2002), which in some quarters is regarded as the South African e-commerce law, addresses the protection of personal information that has been obtained through electronic transactions. According to Clause 50 of the aforementioned Act, the principles for electronically collecting personal information require that, before any such information is collected, a data collector should obtain consent from the individual concerned regarding their personal information. The consent should be in writing and may not be requested electronically. The request should specify why the information is required and what it will be used for. The information should not be made available to a third party without authorisation from the owner of the information. The individual's privacy as regards personal information should be respected at all times.

According to the scope of the abovementioned Act, the data controller may choose to follow the principles outlined above. However, s/he will have a record of this fact in any agreement entered into with the data subject. The data controller must fully subscribe to these principles, and not just selectively. This Act also provides for the protection of critical databases.

3.6.2 Information security to ensure integrity of personal information

Legislators in South Africa have taken the security of personal information seriously. According to Clause 34 of the PoPI Bill No. 9 of 2009, there should be an Information Protection Commission established. Amongst other things, the objectives of this Commission are to, "undertake research into, and to monitor developments in, information processing and computer technology to ensure that any adverse effects of such developments on the protection of personal information of persons are minimised, and to report to the responsible Minister the results of such research and monitoring."

Clause 17 of the PoPI Bill prescribes the following security measures required to ensure the integrity of personal information:

> "The party responsible **must** implement appropriate technical and organisational measures to secure protection of personal information from any harm or unpermitted access. The party responsible should put in place measures to protect personal

> information which is under its control from any within and external threats or risk. The measures need to be updated regularly."

The abovementioned Bill also makes provisions regarding, "information processed by a person acting under authority; security measures regarding information processed by a processor; and the notification of security compromise." All these measures' provisions have been stipulated by the legislators to ensure that information security pertaining to personal information is safeguarded. The National Credit Act No. 34 of 2005 (Part D) places much emphasis on the confidentiality of personal information and consumer credit records. The Companies Act No. 71 of 2008 also makes provision for the preservation of secrecy. The aforementioned Acts are supported by the Labour Relations Act No. 66 of 1995, in particular Clause 91, which deals with the breach of confidentiality, and Clause 126 that deals with the limitation on disclosure of information.

3.6.3 Exemptions and exclusions to provisions of personal information

The PoPI Bill provides for the exemption of processing of personal information as long as certain conditions are met. These exemptions concern the processing of personal information regarding a person's religion or philosophy, race, political persuasion, trade union membership, health and sexual life, criminal behaviour and special personal information. The Information Protection Commission may authorise the processing of personal information by a responsible party even if this constitutes a breach of the information protection principle, but only if:

a) the public interest in that processing outweighs, to a substantial degree, any interference with privacy of the data subject that could result from that processing; or
b) that processing involves a clear benefit to the data subject or a third party that outweighs any interference with privacy of the data subject or third party that could result from that processing.

3.6.4 Enforcement of privacy legislation

As stated in section 3.6 above, the right to privacy emanates from the Constitution of the Republic as part of the Bill of Rights. When one focuses on the enforcement of the privacy legislation, reference to the provisions in the Constitution is unavoidable. Clause 38 in the Constitution deals with the enforcement of rights. Any person or entity whose rights have been infringed "has the right to approach a competent court" and the court may grant "correct relief."

The PoPI Bill, as introduced in Section 3.1 of this study, is an enforcement Act rather than a guiding Act, and that is why it stipulates enforcement measures where there is interference with the protection of personal information. Any aggrieved person may lodge a complaint with the Information Protection Commission in the prescribed manner and form, explaining how the protection of his/her personal information was compromised. The Commission has powers to facilitate settlement between the affected parties. The Bill gives the Commission powers to conduct investigations. However, the Commission may also, after careful consideration, decide not to take any action on a particular complaint.

The Commission may request the judge or magistrate to issue a warrant, "to enter the premises as identified in the warrant, to search them, to inspect, examine, operate and test any equipment found there which is used or intended to be used for the processing of personal information and to inspect and seize any record, other material or equipment found there which may be such evidence as is mentioned in that sub-section." Failure to comply with the provisions of this Act may lead to various penalties. A person found guilty of an offence in terms of this Act may be fined or sentenced to, "imprisonment for a period not exceeding 10 years, or to both a fine and imprisonment."
The next section deals with the recognition of the data messages legislation.

3.7 LEGISLATION PERTAINING TO THE RECOGNITION OF DATA MESSAGES

In South Africa, the ECT Act of 2002 recognises the legality of data messages, providing for the, "admissibility and evidential weight of data messages". The Act also recognises digital signatures. This should be seen as an information security measure for electronic documents and transactions. Amongst others, data message can secured by ecryption and digital signatures.

3.7.1 Legal provisions for data messages

According to the ECT Act (2002), there are legal provisions concerning data messages and the protection thereof. Information is under legal force and effect merely by:

- being completely or partially in the nature of a data message;
- bearing an electronic signature;
- passing the integrity assessment based on the time it was created to its final form as a data message.

In a court case the data in a message should not be rejected as evidence simply by virtue of it being constituted as a data message.

3.7.2 Cryptography

As stated previously, the acceptance of digital signatures by legislation provides information security and integrity for the data messages. The ECT Act of 2002 makes provision for the encryption of the data messages and electronic transactions. Cryptography is the practice of hiding information. Amongst other requirements, companies that are interested in providing cryptography services in South Africa should register with the Department of Communications.

3.7.3 Regulations governing electronic signatures and digital certificates

Establishment of the accreditation authority

In 2004, the Department of Communications in South Africa published the regulations governing electronic signatures and digital certificates. The industry had waited for these regulations for several years and they are now implemented. According to these regulations, an Accreditation Authority will be established to accredit the products or services of those who provide authentication services. The regulations also deal with issues such as the form and manner of applications for product accreditation, the establishment of a public database of accredited products, technical requirements applicable to digital certificates, and seven-year record retention obligations.

In its basic form, an electronic or digital signature and digital certificate are used to verify where a communiqué originated from a particular individual or where a website is operated by a particular person. According to Reinhardt Buys of Buys Attorneys (2004), "the draft accreditation regulations will govern the provision and use of these technologies in South Africa and hopefully establish further trust in e-commerce and promote the use of email and the Internet for commercial and legal reasons." Unlike conventional signatures, digital signatures and certificates are provided by certification authorities like VeriSign (http://www.verisign.com) and Thawte (http://www.thawte.com). It is notable that exceptional software applications that allow the use of digital signatures and certificates have also been developed in South Africa, by Shuttleworth, for example, who established Thawte. Buys (2004) notes that websites of South African banks use digital certificates to authenticate certain pages on their websites. Users of online banking may click on the small padlock icon at the bottom of these websites to view the applicable certificate.

Technical requirements of digital certificates

Chapter VI of the ECT Act (2002) regulates the use of the so-called authentication of "*products and services designed to identify the holder of an electronic signature to other persons".* Whilst encryption technologies are required to be registered in order to avoid criminal prosecution, authentication technologies are subject only to voluntary accreditation. Nonetheless, those authentication providers that fail to apply for accreditation will not be allowed to provide advanced electronic signatures. Regulation 13 prescribes the technical requirements for digital certificates that should be included, namely ITU X.509 compliance. The following section deals with the cyber-crime legislation.

3.8 LEGISLATION PERTAINING TO CYBER-CRIME

The paragraphs below reflect on the literature review pertaining to hacking, industrial espionage and the legislation thereof (ECT Act, 2009).

3.8.1 Hacking

A chapter on the legal framework governing information security would be incomplete without a section on hacking (see Section 2.3.1). A hacker is a person who breaks into computers and/or their systems (Nye, 2013). Schneier (2000:43) reported that the term "hacker" has many definitions, starting from a corporate systems administrator who can make computer systems work. He further notes that the term has been co-opted by the media and "stripped of its meaning". This word used to be complimentary in the past rather than being an insult. However, some authors report that the word "hacker" has become a derogatory term (Mahadeo & Shivaji, 2013; Tiwari, 2013). The word is used in this research in its derogatory form. Maiwald (2004:46) argues that a more correct term would be "cracker" or "criminal". Nevertheless, to comply with the current general usage, the term "hacker" will be used in this study to distinguish those people who intrude into computer systems and/or make such systems dysfunctional and include crackers and computer criminals (Pisaric, 2013).

Crume (2000) and Lawade (2012) claim that some hackers are offended by being bundled together in one group. They hasten to indicate that their rationale for breaking into systems should be appreciated because real hackers break into the system in order to reveal its weaknesses rather than just being destructive. On the other hand, there are those who praise themselves for breaking into computer systems as a way of fighting injustices imposed by governments and the commercial world (Schneier, 2003; Morrison, 2013).

Maiwald (2004:46) claims that studies indicate that most hackers are male, between the ages of 16 and 35, socially solitary, highly intelligent, and technically proficient, although there may be some hackers who may not meet this description. In most instances, hackers have a broad understanding of computers and systems and how they function (Huey, Nhan & Broll, 2013). Equally, some of them understand how protocols work and how protocols can be manipulated to make the computer systems act in a certain way.

3.8.2 Industrial espionage in South Africa

South African organisations are not immune to industrial espionage. According to Mamaila and Green (2002), the South African National Intelligence Agency (NIA) has offered to assist the business community to prevent the theft of its trade secrets. A large number of prominent South African companies, including those who are in mining and ICT sectors, are victims of industrial espionage (Ngobeni, Lubisi & Mahlangu, 2005). A former Director General of the NIA, Mr Vusi Mavimbela, reportedly confirmed these allegations (Mamaila & Green, 2002). The NIA had intercepted information indicating that many South African companies have been plundered of their business strategies. This information is worth billions of Rands (Ngobeni et al., 2005; Dagada, 2013).

Industrial espionage in South Africa is aggravated by the fact that some of these organisations whose information is being looted are using the services of foreign IT firms that steal strategic information and pass it on to their mother countries (Mukwevho, 2009; Ngobeni et al., 2005). Mavimbela emphasised this assertion:

> "Corporate South Africa should wake up to the reality that it was under serious threat from international competitors, some of whom resorted to industrial espionage. You might be wondering why one puts so much emphasis on information and information warfare. The fortunes of nation-states are today governed by who has better access to resources and who can better gain as well as defend strategic information" (Mamaila & Green, 2002).

Foreign companies find it easy to conduct industrial espionage in South Africa because corporate South Africa is very naïve and ambivalent about these issues (Sole & Letsoalo, 2005). Corporate South Africa needs to change its attitude so that it can address the plundering of its intellectual property (Rantao, 2004). This view is corroborated by Mavimbela, who claims that when NIA agents warned some business people that they were being hacked by foreign intelligence agencies, they treated the advice with contempt (Mamaila & Green, 2002). They assumed that the NIA only deals with state security and not business interests. Moreover, some of the companies who were being spied on went to the very same foreign companies who were hacking them and told them that the South African intelligence agency suspected them of industrial espionage (Dagada & Mukwevho, 2013).

3.8.3 Legislation dealing with cyber-crime in South Africa

The ECT Act (2009) contains provisions that deal with cyber-crime and hacking in particular. In the context of this Act, “access” includes the actions of a person who, after taking note of any data, becomes aware of the fact that s/he is not authorised to access that data, yet continues to access that data. Detailed information about the sections in the Act that deal with cyber-crime is presented below.

Unauthorised access to, interception of, or interference with data

As stipulated in Section 86 of the ECT Act, any individual who is not authorised to access particular data, but does so without obtaining the required consent, should be accused of an offence. Again, any such individual who causes interference with the data in any way, such as making any alterations, selling, distributing or performing any unlawful act on the data, should be accused of an offence. Basically, any unauthorised interference with access to an information system is punishable by law.

According to Section 87 of the Act computer-related extortion, fraud and forgery, and states that any malpractice in this regard should be punishable. Examples of such malpractice could be undertaking to restore any damage caused as a result of such actions identified under Section 86, and also initiating non-authentic data to be created with the intention that it should be regarded as authentic. Section 88 shows that any individual who influences anybody to commit the offences covered in Sections 86 and 87 mentioned above, should be punished by law.

Cyber inspectors in South Africa

Legislators and policy formulators in South Africa, noting cyber-related problems regarding patents, trademarks, copyright, privacy and cyber-crime, undertook to legislate measures to deal with these. It is in this context that the ECT Act of 2002 was promulgated and makes provision for the appointment of cyber inspectors.

The Director General of the Department of Communications may appoint any employee as a cyber inspector empowered to perform duties that relate to cyber-crime detection and prevention. Powers of the cyber inspector as reflected in the ECT Act (2002) include monitoring and inspecting “any web site or activity on an information system in the public domain and reporting any unlawful activity to the appropriate authority”. Cyber inspectors will also assess the activities of the cryptography and authentication service providers. Cyber inspectors have powers to inspect, search and seize. They may also request a warrant from a magistrate or judge when this is deemed necessary. The following section deals with the legislation related to malicious code.

3.9 LEGISLATION RELATED TO MALICIOUS CODE

This section deals with the information security concerns of malicious code, its historical overview and the legislation thereof (ECT Act of 2002) (please see Section 2.3.2).

3.9.1 Malicious code as information security risk, threat and crime

The world is confronted by the fast growth of computer viruses and it is difficult to solve the impact of these viruses, in the same way as in the biological field (Thaanum, 2013). Slade (2004) reports that, due to rapid evolution in the corporate and biological world, IBM’s computer virus research task team has extensively investigated possible similarities and differences between biological and computer viruses and epidemiology. The researchers found that the evolution of computer viruses is increasing more dramatically than that of their biological counterparts. Slade (2004) attributes this to the huge growth of computer technology, “as well as homogenisation of computers, operating systems, and software”.

Malicious code/software is one of the information security related problems in most organisations, institutions, government departments and individual home users (Ting & Yi, 2013). According to Maiwald (2004:67), the term “malicious code” refers to computer viruses, Trojan horse programmes, worms and others. Together they are called *malware* (Radha & Mimal, 2012). Malware is a relatively new term in the ICT field and was coined to describe software programmes that are deliberately created to penetrate a system, breaking security, and carrying malicious or destructive payloads. On the other hand, the term malware is sometimes used loosely as a synonym for a virus, whilst the word virus is sometimes used simply to refer to any type of computer problem (Zinszer & Tamblyn, 2013).

Infenedo (2014) declares that viruses are the biggest group of malware, both in terms of quantities of entities and their impact on the information security field. Viruses will therefore receive more attention in this section, but will not be the only type of malware reviewed. It should also be noted that once the attacker launches malware, it will continue to attack without reference to the attacker or user, expanding the attack to other computer systems. It is on this premise that Lai (2013) argues that there is a qualitative difference between malware and hacking tools, kits or scripts that are supposed to function under the hacker's control.

3.9.2 Information security concerns with regard to malware

Malware can attack and damage a computer system's integrity in several ways. Lai (2013) report that viruses are usually defined on the basis of the ability to attach to computer programmes where they will compromise the integrity of applications. According to Slade (2004:1258), claims have been made that 'good' viruses exist. This is problematic because there is sufficient evidence to support the fact that viruses compromise systems and therefore the concept of a 'good' virus is contradictory (Stone, 2013).

Some types of malware have payloads which have the capacity to erase data files or tamper with application data over a period of time (Chahar, Chauhan & Das, 2012). This may lead to the integrity of data being compromised and such data may be rendered useless. Malware is created to use the target computer system as a platform to launch further attacks, without necessarily requiring the instructions of the original author or attacker. This has created problems within intranets, extranets and domains where systems tend to trust each other. It also results in bad will when the system of a particular company inadvertently sends out viruses to other systems. This can also create negative perceptions regarding the adequacy of information security and thus presents a reputational risk to companies (Corrado, 2013).

Slade (2004:1258) claim that malware can compromise programmes and data to such an extent that they are no longer functional and that "malware generally uses the resources of the system it has attacked, and it can, in extreme cases, exhaust [central processing unit] cycles, available processes, memory, communications links and bandwidth, open ports, disk space, mail queues, etc". Malware can also lead to a denial-of-service attack. The aforementioned assertion is supported by Chahar, Chauhan and Das (2012).

3.9.3 Legislation dealing with malicious code

In the bricks-and-mortar commercial environment, consumers are able to check their prospective purchases. However, in the online environment, it is not possible for consumers to “taste the food, try on clothes and test drive a new car” and “for this reason online consumers are given extra protection rights on top of the general and offline consumer protection rights that apply to any specific transactions” (Buys, 2004:138). Chapter 7 of the ECT Act of 2002 requires that online consumers should be protected. Amongst other things, consumers should be protected from malicious code and spam. Consumers should also be protected against unsolicited goods, services or communications. Buys (2004:138) notes that, “in terms of Section 3 of the ECT Act, other consumer protection statutes in South Africa shall also apply to electronic transactions, if and where applicable”.

3.10 ICT RISK REGULATORY ASPECTS IN SOUTH AFRICA

This chapter thus far provided an overview of the information security-related laws in South Africa. Hare (2004) declares that it is compulsory for each organisation to have an information security policy that emanates from legislation. In South Africa, the King III Report (2009:81) compels the Board of Directors to ensure that ICT-related policies are established. Whilst the King II Report solely focuses on the companies that are listed on the Johannesburg Stock Exchange (JSE), King III applies to all organisations notwithstanding the method and form of incorporation or establishment – whether listed on the JSE or not, large and small, public and private. Although the King III Report is not a law, organisations are expected to adhere to its guidelines on an ‘apply or explain’ basis as follows (King III Report, 2009:11):

> “It is the legal duty of directors to act in the best interests of the company. In following the ‘apply or explain’ approach, the board of directors, in its collective decision-making, could conclude that, to follow a recommendation would not, in the particular circumstances, be in the best interests of the company. The board could decide to apply the recommendation differently or apply another practice and still achieve the objective of the overarching corporate governance principles of fairness, accountability, responsibility and transparency. Explaining how the principles and recommendations were applied, or if not applied, the reasons, results in compliance”.

The King III Report's guidelines for information security are contained in seven principles as follows:

Principle 1: The board should be responsible for IT governance. This includes the establishment of IT governance framework, structures and policies.

Principle 2: IT should be aligned with the performance and sustainability objectives of the company. If the information security of the company is properly implemented and tightened, this may pose a risk to the sustainability of the organisation.

Principle 3: The board should delegate to management the responsibility for the implementation of an IT governance framework. Amongst others, management should, on behalf of the board, ensure that information security processes, procedures and standards are implemented to ensure that IT risk is minimised.

Principle 4: The board should monitor and evaluate significant IT investments and expenditure. The investments in IT hardware and software should also cater for the information security related services.

Principle 5: IT should form an integral part of the company's risk management. Information security should be viewed and dealt with as part of the overall risk management.

Principle 6: The board should ensure that information assets are managed effectively. Amongst others, this should include ensuring confidentiality of information, integrity of information, and the availability of information and information systems at all times.

Principle 7: A risk committee and audit committee should assist the board in carrying out its IT responsibilities.

From the above paragraphs, one deduces the importance which the regulatory authorities place on information security. It is on this basis that organisations in South Africa should establish information security policies as a response to the regulatory requirements (Abawajy, 2014). Inevitably, some of these policies will have to address information security in the e-commerce environment. The policy should stipulate in detail, “what must be done, when it must be done, who does it,” and can give insight as to why it is significant to do it (Hare, 2004:933). Other than complying with the regulations, information security regulatory aligned policies should provide consistent operational and behavioural processes (King II Report, 2006:76). Organisations that provide services and/or products to consumers are expected to show some consistence regarding the application of the regulations without prejudice. Chapters 5 and 6 of this thesis indicate how organisations in South Africa can incorporate the regulatory requirements when they develop their information security policies.

3.11 SUMMARY OF CHAPTER 3

This chapter provided a legal framework pertaining to information security in South Africa. The main tenet of this chapter is that information security policies at organisational level should be based on the relevant laws of the Republic. Information security should not solely rely on technical measures. Technical measures dealing with information security should be a consequence of the policies that are derived from the legislation. This chapter explained that there are more than ten laws in South Africa that focus on information security related issues such as trademarks, malicious code, hacking, copyright, patents and privacy.

Some of the South African laws that deal with the above-mentioned information security problems are the following: The PoPI Bill No. 9 of 2009; the Promotion of Access to Information Act No. 2 of 2000; the Companies Act No. 71 of 2008; the Electronic Communications and Transactions Act of 2002; the National Credit Act No. 34 of 2005; the PoPI Bill No. 9 of 2009; the Companies Bill of 2007; the Copyright Act of 1978; the Labour Relations Act No. 66 of 1995; and the Regulation of Interception of Communications and Provisions Communication-related Information Act No. 70 of 2002; as well as the King III Report. The next chapter focuses on the research methodology of this study.

CHAPTER FOUR

RESEARCH METHODOLOGY AND DESIGN GENRE

4.1. INTRODUCTION

In this chapter, a detailed description of the research design is provided, including the description of the research methodology and data collection methods. Qualitative data analysis methods employed in this study are explained. The trustworthiness of the study and the ethical aspects relating to research of this nature is discussed.

The term *genre of design* is deliberately chosen for the purpose of this study instead of the term *design type*. The rationale for doing this was, as part of the research method, to include the researcher's reflexive knowledge of how theory contributes to interpretation and understanding, how ideology, context and politics manifest in the study (Lautenbach, 2005). This stance is supported by Henning, Van Rensburg and Smit (2004) who observes that the term *genre* encapsulates various types of qualitative research more adequately than the terminologies *type* and *format*. Other authors who support this assertion are Bowers, Cohen and Elliot (2013).

In this study, research design was employed as a means to decide what the study purpose and questions would be; what kind of information would be relevant to address specific research questions; and what strategies would be the most appropriate in the process of the enquiry and the analysis of the gathered information (Mouton, 2001; Simmonds & Christopher, 2013). The first question should be not which research methodology to use, but rather what the researcher wants to find out and why. The way in which a study is conceived and executed, and how findings will be analysed, should be inter-connected and grounded in the researcher's philosophical perspective (Lautenbach, 2005; Bowers et al, 2013). Authors such as Henning et al. (2004:30) refer to this as the "epistemological and thus the methodological home of the study". On the other hand, Alvesson and Skoldberg (2000:7) declare that, "it is not methods but ontology and epistemology which are the determinants of good social science". It is on this premise that this study is an interplay between the author's personal philosophical perspective and the empirical findings of the study (Lautenbach, 2005). The way in which the researcher views and interprets the world (the researcher's ontological position) should determine what questions the researcher asks during the study and how the researcher designs the enquiry (Alvesson & Skoldberg, 2000). This view is supported by Scammon, Tamoaia-Cotisel and Day (2013).

4.2 SAMPLING AND PROFILE OF THE ORGANISATIONS

As mentioned in chapter 1, the participants in this study were executives, managers and specialists in information security who are based in 45 South African organisations. In all instances, professionals whose companies' websites are used to conduct financial transactions between buyers and sellers were targeted. The age, gender, qualifications and race of the participants were not recorded as this was not deemed necessary to the study. However, the positions of the participants were recorded as they show the responsibilities and jobs of participants in terms of legal and policy aspects to be considered in the provision of information security in the corporate environment.

It was previously explained that convenience and purposive sampling were used because the abovementioned organisations have a presence, including head offices, in Gauteng and it was economical to interact with them as the researcher is based in Johannesburg. However, certain organisations were purposively targeted because of the value they would add to this study. Other than these organisations, the researcher also liaised with experts based with vendors, at universities, non-profit organisations, and consulting organisations. More detailed information is provided in Appendix A1: Request to participate in the study, and Appendix A2: Profile of the organisations that participated in this study.

This section depicts the context in which this investigation took place. The participating companies/organisations are briefly described here and then classified into different industrial sectors. This will enable readers to contextualise the integration of legal and policy aspects in the provision of information security in these organisations.

Table 4.1: Sampling and positions of respondents

Organi-sation by No.	**Title/Position the interviewee/s**	**Industrial Sector**
No. 1	- Managing Executive of Digital Banking Channels - Head of Internet Channel	Banking
No. 2	- Senior Channel Manager: Cell phone & Electronic Channels - Head of Virtual Channels	Banking
No. 3	- Webmaster for Self-Service Banking - Director of Self-Service Banking - Senior Manager: Integration Strategy	Banking
No. 4	- CEO: Mobile & Transact Solutions - Head of Messaging	Banking
No. 5	- Channel Manager: Mobile Portals	Banking
No. 6	- Executive Head: Mobile Money	Telecommunications
No. 7	- Restaurant Franchise Webmaster	Services Sector
No. 8	- Florist General Manager	Services Sector
No. 9	- Chief Information Officer	Airline Transportation
No. 10	- Senior Information Technology Consultant	Airline Transportation
No. 11	- Information Security Officer	Airline Transportation
No. 12	- Business Analyst	Airline Transportation
No. 13	- Manager: Applications Architecture	Airline Transportation
No. 14	- Webmaster	Airline Transportation
No. 15	- Data Room Supervisor	Online Retail
No. 16	- Supply Chain Manager	Online Retail
No. 17	- ICT Operations Manager	Online Retail
No. 18	- Business Analyst	Airline Transportation
No. 19	- Assistant Director: ICT Infrastructure	Airline Transportation
No. 20	- Webmaster	Airline Transportation
No. 21	- General Manager	Online Retail
No. 22	- Manager: Information Services	Online Retail
No. 23	- Information Security Officer	Online Retail
No. 24	- Supply Chain Manager	Online Retail
No. 25	- Marketing Manager	Cinema
No. 26	- System Administrator	Cinema
No. 27	- Compliance Officer	Hotel
No. 28	- Help Desk Manager	Hotel
No. 29	- Executive Director: Information Technology	Hotel
No. 30	- General Manager: Networks	Hotel
No. 31	- Chief Information Officer	Hotel
No. 32	- Senior System Engineer (Unix)	Hotel
No. 33	- Data Centre Manager	Hotel
No. 34	- Team Leader: IT Security	University
No. 35	- General Manager: Support Services	University
No. 36	- Technical Administrator	Hotel
No. 37	- General Manager: ICT & Knowledge Management	Broadcasting

Organi-sation by No.	**Title/Position the interviewee/s**	**Industrial Sector**
No. 38	- IT Support Senior Manager	Broadcasting
No. 39	- Assistant General Manager: Business Solutions	Online shop
No. 40	- Systems Engineer: Standard Operating Environment	Car hire
No. 41	- Business Process Analyst	Car hire
No. 42	- Manager: ICT Corporate & Commercial Services	Car hire
No. 43	- Senior Systems Programmer	Telecoms
No. 44	- Team Leader: Application Development	Telecoms
No. 45	- Systems Engineer	Telecoms

During the first engagement with the organisations that participated in this study, the commitment was made that by all possible means it would be ensured that their participation in the study was not to their disadvantage (see Appendix A1). Therefore pseudonyms were given to all participants to protect their identity.

4.3 THE RESEARCH DESIGN

The research design was used as a plan according to which information from the study participants was obtained (Welman & Kruger, 2001; Miller, Crabtree, Harrison & Fennell, 2013). The detailed research design is explained in the sections below.

4.3.1 Overview of the research design

Merriam (1998) and Sowan and Jenkins (2013) explain that the research design is a map or plan which guides the researcher during the course of the enquiry. It is a product of several research questions (Kalmbach, 2013; Cresswell, 2007). A qualitative research design was used in this study.

Pluye, Grad and Johnson-Lafleur (2013) and Welman and Kruger (2001) are of the view that positivists and anti-positivists constitute two paradigms about the research design. The positivists advocate for the research design to be determined before data gathering, while the anti-positivists prefer emergent designs (Dixit, 2013; Miller et al., 2013). According to the emergent design, the researcher may amend his or her data gathering methods during the course of the study. In this study, it was decided to use the research design before data gathering (Bertens, Broekhuizen & Naaktgeboren, 2013). This was done so that the research could be conducted within a certain framework and focus. The design that would allow the phenomenon to articulate for itself was chosen. In actual fact, the researcher proceeded within the specific design because a decision was required regarding the study topic, approach and location to the research.

4.3.2 Qualitative research design in the context of this study

Qualitative study is a broader concept which entails multiple kinds of research that will allow researchers to comprehend and describe the meaning of the social phenomena with minimal disruption of the natural setting (Merriam, 1998; Newington & Metcalfe, 2014). There are many types of qualitative research designs (Strang, 2013; Bertens et al., 2013). This study took the form of a generic study (Drabble & O'Cathain, 2014). In this research, the reality of how legal and policy aspects are integrated in information security endeavours in corporate South Africa was constructed through interacting with individuals in their social worlds. This interplay is referred to in section 4.1 as ontology and epistemology.

In this study, the social worlds were 45 South African organisations (see Appendix A2), consultancies, non-profit organisations and universities (see section 4.2). The researcher assumed that meaning regarding the integration of legal and policy aspects in information security is attached to the experiences and perceptions of executives, senior managers, webmasters and information security specialists who were interviewed as part of this study. It is further acknowledged by the researcher that the reality integration of legal and policy aspects in information security in the corporate environment could be mediated through his own perceptions (Merriam, 1998; Drabble & O'Cathain, 2014) (compare section 4.1: "researcher's own ontological position"). The qualitative research design enabled the researcher to comprehend the phenomenon of interest from the participants' perspective rather than his own.

In this study, the researcher was the primary tool for data collection and analysis. Through the fieldwork, several companies were approached, as well as consultancies, non-profit organisations and universities in order to interview relevant people. The purpose of the visits to the aforesaid organisations was to interact with people and observe their behaviour in their natural setting. Documents were collected from the above-mentioned organisations and the functionality and content of the websites of the participating organisations was observed.

4.4 DATA COLLECTION METHODS USED IN THE STUDY

The research made use of generic techniques for qualitative collection and analysis (Kauffman et al., 2012). This study is generic in that it involves many companies and it was not conducted within a bounded system (Merriam, 1998:27). The integration of legal and policy aspects in information security in the corporate environment is not a phenomenon which is bounded, nor is it a case (Merriam, 1998:27). In fact, Welman and Kruger (2001) and De Guinea, Titah and Leger (2013) loosely describe a study of this nature as generic survey research. No experiments were conducted as part of this study and nothing was manipulated in order to observe the outcome of such intervention. This study merely investigates how legal and policy aspects are integrated in the implementation of information security in corporate South Africa.

Interviews, document analysis, and websites functionality and content were used as data collection methods. More detail on the functioning is provided in the sections below.

4.4.1 Interviews in the study – Overview

The interview was an exceptionally appropriate data gathering method for this type of study, and made it possible to collect substantial information pertaining to the types of research questions outlined in Chapter 1. Interviews provided the opportunity to liaise directly with participants in the study, and to collect information directly from executives, managers, webmasters, information security specialists, information security experts, legal experts, and ICT legal experts.

At the beginning of each interview, the purpose of the study was explained to the potential participants and their co-operation requested. Each participant was given a provisional indication of how long the interview would take. The interviewer was candid and honest during the interviews in order to build up trust. Although 56 interviews were conducted in this study, interest was shown in each individual participant and recognition of the fact that their perceptions and experiences about information security were unique.

During the course of the interviews, interviewees were guaranteed their anonymity. They were also encouraged to communicate their genuine opinions, experiences and perceptions without fear of condemnation.

Semi-structured interviews were used because they were more suitable for this study due to the fact that participants came from divergent backgrounds and an interview protocol was available to guide the interviewer (Welman & Kruger, 2001; Ma, 2012). The interview protocol had a list of topics to be addressed (Appendices B1 & B3). Although all interviewees were asked the same questions, the formulation was modified to suit the context and level of the respondent. Interviews were conducted from January 2011 to December 2011. The average length of an individual interview was about forty minutes. The interviews were recorded so that data could later be transcribed and analysed (Ma, 2012).

The researcher intentionally targeted highly experienced respondents in line with what Naimark and Teklina (2011) and De Guinea et al. (2013) refers to as an elite interview and/or an expert interview. Several such interviews were conducted with executives, managers, webmasters, information security specialists, information security experts, legal experts, and ICT legal experts in several organisations. These professionals were either directly or indirectly responsible for the information security in their organisations or client organisations. Calafiore, Dabbene and Tempo (2011), and Ma (2012) describe elite respondents as powerful, renowned and knowledgeable about specific subjects. In the context of this enquiry, the executives, managers, webmasters, and information security specialists provided information about challenges and issues to integrate legal and policy aspects in the implementation of information security in their organisations.

Eleven elite and individual interviews were conducted with information security experts, academics, and ICT legal experts who were not in the corporate environment, but were based in non-profit organisations, consultancies, and universities. Although these people are not in the corporate environment, they provide consulting expertise to companies and many of them are regarded to be thought leaders in the field of information security in South Africa as well as being highly respected internationally. Table 4.2 below summarises the profile of experts who were interviewed using pseudonyms.

Table 4.2: Elite and individual interviews with experts

Name of expert	Title/role of expert	Industrial sector
Expert A	- Lawyer A	Legal Firm 1
Expert B	- Lawyer B	Legal Firm 1
Expert C	- Lawyer C	Legal Firm 2
Expert D	- Lawyer D	Legal Firm 3
Expert E	- Lawyer E	Legal Firm 3
Expert F	- Lawyer F	Legal Aid Clinic
Expert G	- Managing Director (A)	Legal Firm 3
Expert H	- Senior Lecturer	Law School
Expert I	- Researcher	Security Institute
Expert J	- Journalist	Print Media
Expert K	Managing Director (B)	ICT Consultancy and Training Firm

The interview questions that were posed are contained in the Appendices: Appendix B1: Protocol for Semi-Structured Interview: Information Security Practitioners within the Participating Organisation; Appendix B2: An Example of Individual Interview: Information Security Practitioner within the Participating Organisation; Appendix B3: Protocol for Semi-Structured Interview: Information Security or Cyber Law Expert; and Appendix B4: An Example of Individual Interview: Information Security or Cyber Law Expert.

4.4.2 The use of website analysis in the study

In addition to employing individual interviews as a constructive and direct way of determining the integration of legal and policy aspects with the implementation of information security in the South African corporate environment, websites were also used for data gathering. Feng, Ma and Fan (2011) declare that observation (website analysis) as a data collection method has several advantages over interviews. This was proved to be correct during the course of this study. In this study, website analysis enabled the researcher to obtain information about the functionality and content of the websites of the participating organisations and how these websites address the legal requirements pertaining to information security. Secondly, website analysis enabled the researcher to capture certain behaviours that respondents often took for granted. During website analysis, it was possible to obtain information about matters that participants had not been able to describe adequately in the interviews. Another advantage of using website analysis as a data gathering method was that the data gathered was used to verify and complement the information obtained from individual interviews and corporate documents.

During the website analysis, webmasters were not asked to create extraordinary functionality or to upload certain content in their websites. Every attempt was made to maintain the authenticity of the setting to allow website functionalities to be observed as they occurred or the content as it appears. This kind of analysis made it possible to gain insights that might have been missed had special activities been requested. Moreover, website analysis allowed for greater emphasis to be placed on the depth rather than the width of data, thus illustrating the detail, difficulty and subtleties of the normal setting. An holistic perspective was also emphasised, with information security being studied in relation to its context. A website analysis protocol was used to guide the website analysis sessions (Feng et al., 2011). In this study, the researcher used the guidelines appearing in Table 4.3 below. It was not, however, the intention of this study to test and observe the security strength of the websites of the participating companies.

Table 4.3: Analysis of the websites legal compliance

No.	ASPECTS ANALYSES	YES	NO
1.	Does the website have functionality for online payments?		
2.	Does the website have any legal notices?		
3.	Does the website have terms and conditions available as hyperlinks?		
4.	Does the website have liability disclaimers available as hyperlinks?		
5.	Does the website contain legal notices that address the provisions of Chapter 3, Part II and Chapter 7 of the Electronic Communications and Transactions Act of 2002?		
6.	Does the website position and implement legal notices correctly?		
8.	Are the legal notices in the website printable or saveable as required by section 11(3) of the Electronic Communications and Transactions Act of 2002?		
9.	Does the website contain policies that address legal compliance pertaining to websites?		

4.4.3 The use of document analysis in the study

Data was also collected through document analysis in line with Merriam's (1998) recommendations. Data collected through other methods – individual interviews and website analysis – was also evaluated against South African legislation pertaining to information security. These include the following pieces of legislation (as discussed in Chapter 3): the Constitution of the Republic of South Africa of 1996; the Promotion of Access to Information Act No. 2 of 2000; the Electronic Communications and Transactions Act No. 25 of 2002; the RICA, 2002; the Intellectual Property Law Amendment Act of 1997; the Copyright Act of 1978; the Merchandise Marks Act of 1941; the National Archives and Records Service of South Africa Act No. 43 of 1996 (as amended); the National Archives and Records Service of South Africa Regulations of 1997; the Promotion of Access to Information Act No. 2 of 2000; and the Promotion of Administrative Justice Act No. 3 of 2000. During the course of the fieldwork, the researcher collected and analysed documents, policies and legislation pertaining to hacking, interception and surveillance, intellectual property, malware, copyright, trademarks and privacy from all 45 organisations that participated in this study. Several information security related policies from the participation organisations or generic policies within the focus of the study were also analysed, including the ICT Acceptable Use Policy; Information Security Policy; Data Privacy Policy; Access to Information Policy; Interception and Surveillance Policy; Records Management Policy; Electronic Communications Policy; Intellectual Property Policy; and Plagiarism Policy. Other documents collected and analysed include the Records Retention Schedules and Guidelines of the National Archives. Table 4.4 below presents the data collection protocol used to guide the researcher in respect of the necessary documents.

Table 4.4: Document collection and analysis protocol

Area of Information Security	Relevant Policy	Relevant Legislation	No. of Organisations Complying
Hacking			
Malware			
Interception and surveillance			
Intellectual property			
Copyright			
Trademarks			
Privacy			

In line with Merriam's (1998) advice, during the course of the fieldwork and document collections, the value of each document was assessed as a source by determining its relevance. This approach is supported by Pan, Yang and Tang (2012). Most of the documents were requested from the companies that participated in this study and the researcher received most of these documents after providing an undertaking that documents would not be shared and the identity of the company would not be disclosed. Some of the companies that participated in this study regarded information contained in these documents as confidential and of a strategic nature. Appendix C: an Example of a Document Gathered from an Organisation provides detailed information.

4.5 THE USE OF QUALITATIVE DATA ANALYSIS IN THIS STUDY

4.5.1 Overview

Zhang, Zhang and Mi (2012) observe that qualitative data analysis is generally in the mode of written language. It can, however, also entail other forms such as audio-visual recordings or sketches. The focus of data analysis in this study is information obtained from executives, managers, webmasters, information security specialists, information security experts as well as verbal information from academics obtained in individual interviews. Data analysis in this study is also focused on website analysis and documents collected from the organisations that participated in this enquiry.

4.5.2 Data management and reduction in this study

Due to the fact that 56 interviews were done and extensive documentation was collected from the participating organisations, it became apparent that the raw data should be selected, focused, simplified and transformed (Hassan & Sabry, 2013; Zhang et al., 2012). This was done by sub-dividing the raw data into units (Alazab & Venkatraman, 2013). These units comprised portions of the respondents' verbal responses. Portions of the participants' verbal expressions were initially coded (Haahr, Norlyk & Hall, 2014). Portions from transcribed interviews were compared with portions of website analysis, verbal expressions recorded in the field notes and documents collected from the participating organisations. That is why cross-analysis was used in order to go further than a categorical integration when drawing inferences (Saeedi & Doolen, 2012). The researcher condensed the large sections of raw data by reducing it to certain categories, and thus began to draw conclusions from the start of the data gathering process.

4.5.3 Methods of data analysis in this study

Data analysis in this study has been presented in the mode of descriptive printed words. Serrano, Rovatsos and Botia (2013) observe that the intention of data analysis is to acknowledge components of meaning. In this study, reading each sentence of the raw data that was attained through literature review and several interviews identified units of meaning.

The data acquired from individual interviews was analysed using open coding. A rigorous comparative method was applied to analyse data within and between the research interviews. Content analysis was also used to analyse the interview data. This process entails the concurrent coding of raw data and the composition of categories.

Data was analysed with the intention of identifying frequent patterns and establishing categories; these were compared with the literature, information security policies, and legislation. These categories were used to answer research questions. Data obtained from website functionalities and content was also analysed with the aim of identifying common patterns and formulating categories. Content analysis was used to analyse field notes compiled during website analysis sessions. Common patterns and themes were identified and categories established.

Data collected through interviews and website analysis was analysed by comparing it with the South African information security related legislation and policies collected from the participating organisations. Content analysis was also applied to analyse the legislation and policies. The data gathered was weighed against existing literature. The results were contextualised to the South African legislative framework and corporate environment. An in-depth account in a narrative form has been used in this study for reporting the findings of this enquiry.

4.6 THE TRUSTWORTHINESS OF THE RESEARCH

At the beginning of the fieldwork, participants were assured that their identities would not be revealed. In instances where mentioning names was unavoidable, written consent was obtained from the relevant individuals and organisations. The following sections explain the steps embarked on to guarantee the trustworthiness of the study.

4.6.1 Measures to ensure validity of the study

According to Saeedi & Doolen (2012), there are different views of validity. Derrida (1997:31) observes that several things, including validity, "do not have definable meaning". The following discussion illustrates how validity was established regarding the integration of legal and policy aspects in the implementation of information security in the South African corporate environment.

What is internal validity

Internal validity deals with how the research findings tie in with the reality (Saeedi & Doolen, 2012). In this study, the research findings were matched with the reality of information security implementation in corporate South Africa. The following themes, as espoused by Merriam (1998), and Simon (2013), demonstrate the measures that were taken to ensure the validity of the study.

(a) Triangulation

This study employed multiple data collection techniques to establish how legal and policy aspects were being integrated in the implementation of information security in corporate South Africa. Data was gathered by applying three data collection methods: semi-structured individual interviews, website analysis, and document analysis. The use of numerous sources also satisfied the validity of this study. These sources include interviews with executives, managers, webmasters, information security specialists, information security experts, and academics. Multiple data analysis techniques were employed in the study and assisted in promoting the principles of validity. Data analysis methods used include open coding, content analysis and document analysis.

(b) Member checks

Organisations and people participating in this study were given the opportunity of examining the evolution of the research report as it was being written up. This was done to make it possible for them to identify information which may not be an accurate reflection of what was said, read and/or observed during the fieldwork. Further discussions often took place between the participants and the researcher to ensure that the findings of the study were valid. Furthermore, some research participants occasionally enquired about the progress of the research report.

(c) Long-term website analysis

The websites of the participating organisations were analysed from January 2011 to December 2011. During the website analysis sessions, the researcher took notes relating to the content and functionalities of the websites.

(d) Peer examination

During the course of this study, ideas and findings were subjected to peer review and discussion to establish credibility in the study. This was achieved by publishing the following papers:

- Dagada, R., Eloff, M.M., & Venter, L.M. (2009). *Too many laws but very little progress! Is South African highly acclaimed information security legislation redundant?* ISSA 2009 Conference. University of Johannesburg, 6-8 July 2009.
- Dagada, R., & Eloff, M.M. (2013). Integration of policy aspects into information security issues in South African organisations. *African Journal of Business Management*, 7(31), 3069-3077.

In 2009, the researcher presented a paper emanating from the literature review and pilot fieldwork of this study at the School of Computing 2009 Post-Graduate Symposium, held at the University of South Africa on 14 September 2009, where the paper was rated as the best doctoral study presentation. In this way, the researcher was able to obtain invaluable feedback from both the academics and professionals within the field of study.

External validity

The predicament faced by the qualitative researcher by and large revolves around the justification for generalising the findings of that specific portion of research to some wider context (Kwuida & Schmidt, 2011). According to Klimova and Mikheyenkova (2012), transferability is used to establish the applicability of the findings to other contexts. It was mentioned in chapter 1 that this study may impart crucial insights into the future implementation of information security by South African organisations, boards of directors, information security practitioners, e-commerce participants, ICT executives and those in charge of policy formulation. Although the organisations selected for this investigation are situated in South Africa, most of them operate worldwide. The findings and recommendations of this study may therefore be very useful and applicable to similar organisations globally.

For the purpose of this study, external validity also means that there is sufficient narrative of the context of the study to allow readers to match it up to other contexts. To enhance the ability of the reader to make the findings of this qualitative study transferable to other contexts, the following strategies as illustrated by Merriam (1998:211) were applied:

a) Rich, thick description

Since adequate description about organisations and individuals that participated in this study has already been provided, the reader should be able to determine how directly their own situations match up to the research setting and whether findings can be generalised. Section 4.2 describes the research sites as fully as possible by:

- Providing the industrial sector of the organisations that participated in this study;
- Providing positions of professionals who participated in this study. The job titles of participants would make it possible for the reader to ascertain the trustworthiness of the respondents that provided information during the interviews; and
- Evaluating the findings of this research against the literature. The literature also contains what is happening in terms of information security in other countries and thus readers could compare the South African context with other settings in other countries.

b) Multisite design

This study involved 45 organisations and the fieldwork was therefore conducted in a number of different locations, including, but not limited to, in the banking, transport, online retail, hotel, broadcasting and telecommunications sectors.

4.7 ETHICS

Ethical considerations were observed in this study although some readers may not view this work as being sensitive research. Research participants, both at organisational and individual levels were asked to take part in this study. The requests were conveyed through e-mailed letters (Appendix A1: Request to Participate in the Study). Almost all research participants who agreed to be involved this study approved in writing.

All interviewees consented formally to their participation in the study. They also consented to the recording of conversations during data collection. The researcher then coded the audio-recorded interviews, using pseudonyms, and stored the recordings in a locked facility. Interviewees were also at liberty to withdraw from the study at any time and were not required to provide a reason. The researcher undertook all measures to ensure that organisations and individuals participating in the study are not caused any harm by doing so and for that reason; pseudonyms were used to safeguard the identity of the participants and to ensure that any information revealed, either personal or professional, would be treated as completely confidential.

There were, however, benefits for organisations and individuals for being involved in this enquiry. These included short presentations on preliminary and final findings, conference papers and articles with regard to this study.

Ethical clearance was obtained from the College of Science, Engineering and Technology’s Ethics Clearance Committee (Ref: 062/RD/2013).

4.8 SUMMARY OF CHAPTER 4

This chapter started with an overview of the research context, followed by brief descriptions of the organisations participating in this study. This information was provided to enable readers to contextualise the implementation of information security and its integration with legal and policy aspects in these organisations.

It was stated that this study employed a generic qualitative methodology. The interviews, website analysis and document analysis as data collection methods used in the research were discussed. It was explained that qualitative data analysis was employed in the context of this study. Trustworthiness and ethical considerations were discussed.

Chapter 5 presents the findings of the research which is expected to demonstrate how South African companies are employing the provisions of these laws in their information security endeavours.

CHAPTER FIVE
FINDINGS OF THE STUDY: FINDINGS OBTAINED FROM INTERVIEWS

5.1 INTRODUCTION

In the previous chapter, the study focused on the research design of the study. Details of the research approach and procedures were provided. This chapter discusses the findings that were obtained through interviews. It may be noted that throughout the chapter, the researcher offers his own interpretation and understanding of the data. This is in line with the selection of the ‘genre of design’ as stated in Chapter 4 (section 4.1). The author also stated in the Disclaimer which appeared at the beginning of this thesis. The IANAL principle of, “I am not a lawyer”, clarifying that this research is not a legal study but rather an information systems study. These findings address the research questions and are presented in categories and sub-categories.

Categories and sub-categories of the findings obtained through interviews were generated by analysing all the interview transcripts. Interviews addressed three main topics: the attitude of corporate South Africa towards information security legislation; the manner in which organisations in South Africa integrate legal aspects into their information security policies; and users’ knowledge regarding information security policies. Several sub-categories were derived from these three main categories. This study found that the participation of some Boards of Directors in the establishment of the ICT policies was minimal. Section 5.2 discusses the findings in more detail.

Table 5.1 below summarises the analysis and shows the relationship between categories and sub-categories.

Table 5.1: Summary of Analysis showing the Relationship between Categories and Sub-categories

Data collection technique	**Main category**	**Sub category**
Individual interviews	Attitude of corporate South Africa in the study towards information security legislation	• The Board of Directors is not involved in the formulation of information security policies • Very few organisations in South Africa incorporate legislative requirements in their information security policies • Government slowness in implementing information security laws impacts on the corporate environment's attitude towards legislation
	The manner in which South African organisations integrate legal aspects in their information security policies	• The delegation of trademark responsibilities is not well defined • Legal provisions to fight cyber-crime are redundant • Legal provision that deals with unsolicited communication has a serious loophole • South African Copyright Law is outdated • The Implementation of the Privacy Bill has been delayed • The Patents Law is ineffective • The provisions regarding the prevention of hacking and malicious code are difficult to implement
	The level of users' knowledge of information security policies	• Users have elementary knowledge of information security policies • The organisation's seriousness towards its policies affects users' knowledge • Information security policies awareness programmes are superficial • Users are suffering from compliance fatigue

Each of these sub-categories will be discussed in more detail.

5.2 FINDINGS OBTAINED FROM INTERVIEWS

Although only 45 organisations participated in this study, 56 interviews were conducted. Some of the interviewees were not employed in the 45 organisations that participated in this study but are information security experts based in law firms, institutes, universities and media houses (see Table 4.2). Interviews yielded three main topics: the attitude of corporate South Africa towards information security legislation; the manner in which organisations in South Africa integrate legal aspects in their information security policies; and users' knowledge regarding information security policies. Several sub-categories were derived from these three main categories. Appendix B provides information on the following documents:

- Appendix B1: Protocol for Semi-Structured Interviews: Information Security Practitioners within the Participating Organisation;
- Appendix B2: An Example of an Individual Interview: Information Security Practitioner within the Participating Organisation;
- Appendix B3: Protocol for a Semi-Structured Interview: Information Security or Cyber Law Expert, and
- Appendix B4: An Example of an Individual Interview: Information Security or Cyber Law Expert.

5.2.1 Attitude of corporate South Africa in the study towards information security legislation

This study found the attitude towards the legal aspects of information security in the organisations that participated in this study to be negative. It was found that the Board of Directors in most of the companies that participated in this study did not provide leadership in the formulation of information security policies. Analysis of the findings shows that some organisations in South Africa do not incorporate the requirements of relevant legislation into their information security policies.

The Board of Directors is not involved enough in the formulation of information security policies

This study found that the involvement of some Boards of Directors in the development of the information security policies is minimal or non-existent. This is in conflict with the spirit of good corporate governance as espoused by the King III Report (2009). This was confirmed by a Senior Lecturer (Lecturer A), who is an expert in information security law in the Law School of a prominent South African university: "*King III has more IT governance provisions. IT governance and security are the responsibility of the Board of Directors. According to the King III Report, IT security is an important element of the overall business efficiency and sustainability.*"

This study found that policies in all 45 organisations that participated in this study were actually approved at the Chief Information Officer's (CIO) level. The CIO would convene an

ICT Steering Committee comprising representatives from various departments. The problem is that most of these representatives are not in very senior positions. This indicates that some organisations do not appear to take information security seriously. However, according to the King III Report, information security policies should be approved by the Board and the IT Steering Committee should be chaired by the Chief Executive Officer (CEO); furthermore, "*all Group Executives are expected to serve on the IT Steering Committee.*" Therefore, flouting this provision demonstrates deviance from the King III compliance requirements.

During the interview with the Corporate Governance Senior Lecturer, reservations were raised with regard to certain wording in the Draft King III Report: "*There is somewhere where it says that legislation is not the answer, but the international guidelines such as COBIT or ITIL may be used to measure the satisfactoriness of the organisation's information security. It seems the message they wanted to communicate was that legislation only is not adequate and thus international guidelines and standards should be used. That is why the section was concluded with the phrase that says that it may not be possible to have one size fits all. I had hoped they would change that wording in the final King III Report; but unfortunately they didn't, despite our submission. The problem is that, that assertion would make the IT professionals and information security practitioners more cynical about the legislation*". This gives cause for concern, since South Africa is a constitutional democracy and the rule of law should be respected.

Very few organisations in South Africa incorporate legislative requirements in their information security policies

Legislation in South Africa has a major impact in policy formulation. An information security legal expert (Lawyer A) who participated in the study observed that: "*The problem is that very few IT security experts and practitioners are conscious about this. Technology people are more familiar with the standards; unfortunately there is a myriad of legislation and governance internationally and in South Africa*." In South Africa, in particular, one of the crucial pieces of legislation is the ECT ACT (2002). This Act deals with the removal of legal barriers to electronic transactions and provides an information security framework for both the merchants and buyers. Lawyer A continues: "*You would expect most information security practitioners to be familiar with sections that deal with security related aspects in this Act, but unfortunately very few security experts and practitioners incorporate the Act's* *security requirements in their IT policies. I really think this is highly irregular because it exposes consumers who use the websites of the companies that are not integrating the requirements of the Act for e-commerce purposes.*"

The Johannesburg-based Managing Director A of an IT legal firm concurred: "*One of the observations that I have made is that people buy batches of the policies and they do ISO compliance, for instance '27000' and they will immediately implement those policies rather than drafting the policies based on legislation*." Most IT departments are aware that they should have information security policies but they do not have the awareness to actually make the policies relevant to their own organisations, while also adhering to the legal requirements of the South African laws; instead, "*they'd rather purchase just broadly generated policies and apply those.*" This means that some corporate information security executives are not diligent in the execution of their information security mandate. In addition, they are lax, lack commitment and are characterised by an unprofessional demeanour. This account of information security professionals and their approach to their vocation permeated overwhelmingly during the data collection stage.

During an interview with the Information Security Officer who works for an online bookseller, it was indicated that neither their legal department nor any outside lawyers were involved in four of their information security-related policies and there was no effort to ensure that these policies integrate the legislative requirements. However, it was emphasised that the drafting of their Records Management Policy and Data Retention Schedule was guided by the legal requirements.

A Senior Systems Programmer in one of the biggest mobile telecommunications networks in South Africa and the African continent confirmed that when the IT department drafts the information security policies, they, "*don't consciously look at the legislation and try and match that scientifically against, for example, the Promotion of Access to Information Act*." However, interestingly, it was noted that they, "*relied on the legal department to do that and I think to some extent they did review that and made sure that it was compliant to legislation*." The respondent was not certain whether the legal department did ensure that the policy complied with legislation.

Government slowness in implementing information security laws impact the corporate environment's attitude towards legislation

It was revealed that the attitude of corporate South Africa towards the implementation of the requirements of information security laws is partly affected by the manner in which government performs its responsibilities towards the implementation and improvement of the legislation. Certain provisions in the ECT Act, 2002 have not yet been implemented by the time of writing up this research, despite the fact that the legislation was promulgated already in 2002. Amongst others, this pertains to the appointment of the Cyber Inspectors (Cops). The Head of Messaging in one of the four largest South African banks argues that that Cyber Inspectors in South Africa are largely found in the banks and other organisations. South African banks have dedicated teams of information security professionals who 'combat' Internet-related crimes. After noticing clients' concerns regarding Internet and Cell Phone Banking crime, banks have responded forcefully to crime, and with superiority, in order to prevent financial losses and reputational damage. The Cyber Cops in the banking industry are removing phishing and spoofing websites whilst suspicious emails are blocked before they reach the targeted victim. This observation was supported by a Managing Executive of Digital Banking Channels in another Bank: "*We ensure that we have got monitoring systems, behaviour pattern analysis, and early warning systems. For example, if a spoofing site is picked up worldwide on the Internet or a phishing email goes out, we typically shut the site down within 45 minutes to two hours. It doesn't matter where it sits in the world*." Banks are also available 24 hours a day to help their customers in cases where they suspect their Internet Banking accounts are being defrauded. Customers can phone the contact centre, "*and there is also a button on the Internet banking screen that says "do you want to report a fraud incident", press the button – they will close your account immediately"* (Managing Director A).

A Head of Virtual Channels in one of the banks asserted that there are times when Cyber Cops in South Africa literally prevent money from leaving the Internet Bank accounts fraudulently. They also ensure that transactions via Internet Banking are undertaken in an encrypted environment. It is not possible for criminals to intercept encrypted transactions. It was also found that banks were more compliant with regard to the information security aspects of the legislation than all other industrial sectors that participated in this study. A researcher attached to a security institute argued that the South African banks had no choice but to comply with the legal aspects of information security: "*They are however motivated by business considerations rather than solely being loyal to what the legislation prescribes. Companies in other industrial sectors don't have huge volumes of transactions across the Internet like the banking sector. Consequently, they have very little interest in establishing organs like SABRIC (South African Banking Risk Information Centre) or establishing their own sophisticated teams to fight Internet related crimes*".

The Head of Enterprise Information Architecture at a hotel group concurred: "*We work with the government through the Business Against Crime initiative, but the government should take leadership when it comes to information security crimes, otherwise companies in South African will end up operating paramilitary entities and that is not good in a constitutional state; I mean we are not in the business of securing the country; we are hoteliers. You can argue that the government is actually breaking the law by delaying the implementation of certain aspects of the Electronic Communications and Transactions Act*". The registration of cell phone SIM cards, as required by law, was done seven years after the promulgation of the RICA, 2002. Criminals in the Internet sphere are becoming highly sophisticated and the government should ensure that the legislation is updated and implemented in line with the changing requirements. A lawyer (Lawyer B), who was interviewed in this study, observed that: "*Corporate South Africa will continue to treat legislation with disdain as long as the government itself does not appear to be carrying out its part of the legal requirements*". It is on this basis that it may be concluded that failure by the government to appear to be taking its own laws seriously has negative ramifications in relation to the attitude of corporate South Africa towards information security legislation.

5.2.2 The manner in which South African organisations integrate legal aspects in their information security policies

Findings contained in this section reflect that the delegation of trademark responsibilities is not well defined; some legal provisions to fight cyber-crime are not implemented; legal provisions that deal with unsolicited communication have serious loopholes; South African Copyright law is obsolete; the implementation of the Privacy Bill has been delayed; the Patents law is ineffective; and the provisions regarding the prevention of malicious code are difficult to implement. The main category and sub-categories of these findings are illustrated in Table 5.1 above.

The delegation of trademark responsibilities is not well defined

Even in organisations where the protection of trademarks has been incorporated in policies; the responsibilities of implementing them are not well defined and this has the potential of rendering the policy redundant. In a particular car rental company, the IT Department has initiated the establishment of the Intellectual Property Policy which, amongst other things, caters for the protection of trademarks: "*Although we have this kind of policy, it is important to stress that we don't regard things like websites and trademarks to be part of the IT Department's domain; they actually belong to the Corporate Communications and Marketing Department. The problem with our Corporate Communications and Marketing Department is that it is very lousy*"[1]. When scrutinising the abovementioned Intellectual Property Policy, it was revealed that it did not specifically delegate the responsibility to any particular department. The researcher raised this issue with the interviewee (Business Process Analyst) and the response was that certain things are common sense. The interviewee further argued that Corporate Communications and Marketing know that they are responsible for the websites and trademarks: "*That's what they get paid for, otherwise they are redundant*". This lack of clear delegation of authority has other serious ramifications. The researcher established that even the top management in a certain hotel group viewed the websites, Intranet and the related organisational trademarks that appear in these sites as being the responsibility of the IT Department. This was regarded by the researcher as being highly problematic because then these issues, including the budget thereof, are misplaced.

In a particular airline company, the IT Department found itself involved in a legal dispute pertaining to the domain name which was illegally taken by another company: "*To us this constitutes a battle for the trademark since our former Internet Service Provider illegally sold our website to some US company. Our website constitutes a very famous brand in South Africa and we're going to fight this vigorously. The problem is exacerbated by the fact that our own legal department is not knowledgeable regarding ICT related matters. The matter has since been referred to a legal firm which specialises in Information Technology law; but*

[1] Interview with the IT Support Senior Manager (and her colleague Business Process Analyst)

you would have expected our lawyers to give instructions to this legal firm, but they are unable to do so due to lack of knowledge. So they have asked the IT Department to give the instructions; this is highly improper. But still, we are engaging those outside lawyers and someone has to do this. A formal complaint has been submitted to the World Intellectual Property Organization's (WIPO) Arbitration and Mediation Centre in Geneva, Switzerland[2]", said the Senior Information Technology Consultant. The researcher was subsequently informed that the company won the case and they got their domain name back. It was of interest to the researcher to note that even the Legal Department could not carry out their responsibilities and that the IT Department had to become involved in legal matters.

During an interview with a Data Centre Manager at a certain hotel, the issue of the lack of a clear mandate regarding Internet-related trademarks again emerged: "*Last year, we received a communiqué from a certain organisation which deals with domain name dispute and registration in Asia. They alleged that they have received an application from a certain company requesting to register domain names that closely resemble our organisational name and trademark. It was not for the first time that this has happened. The problem is that each time matters of this nature arise; the IT Department is expected to take leadership instead of the Legal and Communications departments. This is grossly wrong, and it is something that we shall never win however we debate the matter*".[3]

Some legal provisions to fight cyber-crime are not implemented

Some of the South African legal information security provisions were highly acclaimed when they were introduced, but unfortunately, they have not yet been implemented. These include provisions to prevent viruses, hacking, and industrial espionage. Provisions to fight against such IT-related crimes are contained in Chapter 8 of the ECT Act (2002). Hacking, industrial espionage, viruses, spam emails and other cyber related crimes are characterised by an unauthorised access to, interception of, or interference with data and thus they are supposed to be tackled by cyber inspectors. A Senior Lecturer who specialises in information security law explained that the provision for the cyber police is, "a*rticulated in Chapter 12 of the Electronic Communications and Transactions Act*." It is unfortunate that this provision has not yet been implemented, even though the Act was passed more than eleven years ago.

[2] Interview with the IT Support Senior Manager.

[3] Interview with the General Manager: IT Support Services.

After realising that cell phones were contributing to criminal activities, law-makers in South Africa established the RICA Act, 2002. Amongst other things, this Act stipulates that the buyers of pre-paid SIM cards should be registered by cell phone network operators so that the law enforcement agencies could identify them if and when their cell numbers are used to plan or commit a crime. A legal expert (Lawyer C) indicated that, "*With effect from 1st of July 2009, the relevant sections of which requires the mobile network operators to register and verify the identity of the 'pay-as-you-go' subscribers came into effect. Parliament has given the network operators 18 months in which to comply. To me this is highly problematic because during the course of these 18 months cell phones will continue to be used to commit crimes.* This view was supported by a General Manager: Group Information Services who is based at a broadcasting company, and viewed this as a blow in terms of dealing with crime: "*The delay in implementing this requirement is not justifiable, especially when you consider the fact that the Act was passed in 2002*."

One is not sure if the arrests of mobile banking fraudsters which took place in July 2009 had anything to do with the eagerness of the government to prevent crimes that are perpetrated with the assistance of cell phones. During an interview with a journalist who wrote a front page newspaper article regarding the aforesaid arrests, it was indicated that: "*It seems the SAPS [South African Police Services] are making some ground-breaking progress regarding the SMS [mobile] banking related crimes. Security breaches have been taking place between the banks and SMS banking customers. Two members of an alleged sophisticated SMS Banking fraud syndicate were arrested on the 9th and 10th July 2009 respectively. One of the suspects holds a Bachelor of Science Engineering Degree and works for a leading mobile network operator in South Africa*". The syndicate would block and delay SMS (Short Message Service) notifications from the banks to the relevant account holders whose accounts were then being plundered by the criminals. The network operator employee was responsible for diverting messages to their own cell phones. That is how they would get access to the victim's details such as the account number and user names. They would then get the OTP (One Time Password/PIN) from the diverted SMS and thus they would obtain easy access to the targeted account. An Executive Head: Mobile Money in a mobile telecommunications network operator confirmed that the police would have used the provisions of the RICA Act of 2002, because it allows them to work with the mobile network operator to intercept communications of people suspected of being involved in criminal activities.

Chapter 10 of the ECT Act, 2002 advocates strongly for the establishment of the Cryptography Providers. This is one of the legal measures to prevent IT-related crimes by, amongst others, legitimising electronic signatures. The Manager: Applications Architecture at an airline transportation company commented that, "*The ECT Act recognises and encourages the use of reliable electronic signatures which are referred to as AES (Advanced Electronic Signature). This can be seen as some sort of SABS (South African Bureau of Standards) approval stamp. The AES's should only be issued by an ASP (Authentication Service Provider) and for several years the government has not established the ASP*". This has been highly problematic in terms of information security because AES provides authenticity, credibility and security of digital transactions and information. After nearly eleven years had lapsed since the abovementioned Act was passed, the government eventually appointed a South African-based cryptographic security provider, LawTrust. Whilst the government should be commended for the aforesaid appointment, the delay in doing so, and thereby ensuring compliance, does not encourage South African organisations to abide by the law.

Legal provision that deals with unsolicited communication has a serious loophole

Unsolicited emails, famously known as spam emails, are addressed in Chapter 7 of the ECT Act, 2002. This chapter of the Act deals with consumer protection. Spam emails are dealt with in Clause 45, which prohibits unsolicited commercial communications to the consumers. However, during the interviews, interviewees indicated that this prohibition is not effective. Sellers of goods, products and services use a loophole in the Act to send chains of unsolicited messages to consumers. The Head of Internet Channel in a particular bank noted: "*The Act says the sender should give the recipient a choice to stop the subscription. However, consumers are uninformed and thus they are swamped with spam emails. In reality, the first email that is sent is unsolicited, but it is legal because it gives the recipient an option to opt out. Usually, recipients don't opt out and thus the subsequent emails cannot be defined as unsolicited because the consumer is deemed to have opted to receive the adverts since he did not opt out. This is entirely within the law*." The problem is that most banking clients and others in South Africa have received unsolicited emails with viruses and spyware attached. After several years, the government has now, to some extent, dealt with this legal loophole through the Consumer Protection Act No. 68 of 2008.

South African Copyright Law is out-dated

During an interview with a copyright lawyer (Lawyer C), the lawyer declared that copyright in South Africa is a major problem because it was passed in 1978 before the new democratic constitution, before the onset of the WWW (World Wide Web) and even before the Internet was used for commercial purposes. South Africa is unfortunately one of the leading countries in terms of the level of illegal copying of digital material. Copies of several movies may be found being sold in Johannesburg streets long before they come out on DVD. A prominent film maker in South Africa, Leon Schuster, incurs significant losses due to piracy: "*Interestingly, you'd have noted in the media that the South African law enforcement agencies were able to arrest and confiscated the property of Vedakumary. She was arrested under the Prevention of Organised Crime Act in March 2007.*"[4] On 11 March 2009, the Pretoria Commercial Crimes Court ruled that the valuable property of Ms Vedakumary should be seized. This was the first time in South Africa that private property of an alleged counterfeiter had been seized by the Asset Forfeiture Unit (AFU). The luxury residential property was auctioned: "*According to the abovementioned Act, the proceeds of the sale should go to AFU's Criminal Asset Recovery Fund to fund law enforcement activities*."[5] The law enforcement agencies should be commended for this achievement. Other than the Prevention of Organised Crime Act*, "other related pieces of legislation which are relevant to the digital copyright related problems are the Copyright Act of 1978, and the Intellectual Property Laws Amendment Act of 1997. The problem with the Copyright Act of 1978 is that it is very old and was established long before the Internet was used for commercial purposes. The Legislature should ensure that South African laws are regularly updated to meet the requirements of the changing business environment.*"[6]

The Implementation of the Privacy Bill was delayed

Privacy is catered for in myriad laws – starting with the Constitution of the Republic of South Africa No. 108 of 1996. Other pieces of legislation that deal with privacy include the PoPI Bill No. 9 of 2009, ECT Act of 2002, and the Promotion of Access to Information Act No. 2 of 2000. The nature of a policy that deals with privacy will depend on a particular company. Every company is expected to include the principles of the above-mentioned pieces of

[4] Interview with Lawyer D.

[5] Interview with Lawyer E.

[6] Interview with Lawyer B.

legislation into their privacy policies. "*In actual effect, almost all of the IT security related policies in an organisation should inevitably address the privacy issue; but my observation is that this is not always the case in corporate South Africa. When it comes to the protection of personal information, the government intended to introduce a piece of legislation specifically for this. Unfortunately, this law has not yet been passed despite the fact that a Bill*[7] *has been available since 2009. This Bill contains all the right things in terms of the protection of personal information; for example, it agitates for the establishment of the Information Protection Commission*[8]*".* This Bill was eventually signed into law on 27 November 2013, as the PoPI Act No. 4 of 2013. It is expected that companies will be given at least 12 months in which to comply with this law. Fieldwork pertaining to this study was already completed.

The Patents Law is ineffective

The legal protection of patents in South Africa is derived from the Patents Act No. 57 of 1978 and the Intellectual Property Laws Amendment Act No. 38 of 1997. *"These are some of the laws which were passed long before the Internet was used for commercial purposes"* Lawyer B stated that the Patents Act is one of the most controversial pieces of legislation in South Africa. Chapter 5, Section 25 of the Act states that software patents cannot be patented in South Africa: "*There are several intellectuals who support the Act in terms of forbidding software patents in South Africa. I am against this provision; I feel very strongly that software inventions are part of one's intellectual property and thus they should be patented. If we deny software producers the right to register their patents, it may lead to lower levels of inventions in the software arena. On the other hand, how do you attract foreign direct investment from the software industry if you are going to deny firms the right to register their patents?"*[9] This may have unintended consequences in terms of foreign investment by IT companies in South Africa. There is some irony in that, although the Act says computer programmes cannot be patented, companies and individuals are actually registering patents in the software domain: "*It may be because the law is toothless or officers in the government companies and patents registration agency, the Companies and Intellectual Property*

[7] South Africa. An Act/[Bill] to promote the protection of personal information processed by public and private bodies; to provide for the establishment of an Information Protection Commission; and to provide for matters incidental thereto. Pretoria: The Department of Justice and Constitutional Development.

[8] Interview with Lawyer E.

[9] Interview with the Senior Lecturer.

Commission (CIPC) are not familiar with the provisions of the law."[10] Alternatively, there may be some loopholes that companies are manipulating to get their patents registered and this violates intellectual property requirements.

The provisions regarding the prevention of hacking and malicious code are difficult to implement

The provisions for the prevention of hacking are contained in Chapter 8 of the ECT Act, 2002. Hacking falls under the definition of cyber-crimes because it is characterised by unauthorised access to, interception of, or interference with data: "*Industrial espionage, which is very rampant in South Africa, is also within the definition of the ECT Act. Hacking, industrial espionage, spam emails, and other cyber-related crimes are supposed to be tackled by the cyber cops or rather cyber inspectors*"[11]. This provision is articulated in Chapter 12 of the ECT Act, 2002: "*Whilst this provision has been highly praised by IT and information security professionals, it has unfortunately not yet been implemented*".[12]

The prevention of viruses and other forms of malicious code is provided for in the ECT Act, 2002 in Chapter 8, which deals with cyber-crime. Viruses constitute unauthorised access to, interception of, or interference with data. In other words, sending viruses is a crime since doing so constitutes unauthorised access, interception, and/or interference with data. *"The case law in South Africa does not yet have examples of cases that are related to viruses and other kinds of malicious code. However, cases that relate to malicious code-related crimes are happening in South Africa, especially in Internet banking".*[13] This is done through pharming. This is where viruses are transmitted via infected emails or downloads: "*The virus directs Internet banking users to a false website that looks like the genuine one in terms of design and the user's identification details are captured".*[14] It seems that the unavailability of the cyber inspectors in accordance with the provisions of the ECT Act, 2002 is also a major problem with regard to virus prevention: "*The law enforcement agencies in South Africa*

[10] Interview with Lawyer E.

[11] Interview with Lawyer F.

[12] Interview with the Senior Lecturer.

[13] Interview with Lawyer F.

[14] Interview with a Researcher in a Security Institute.

haven't successfully prosecuted any person for this kind of criminal activities".[15] At organisational level, the policy that usually deals with spam emails and viruses is the ICT Acceptable Use Policy. In reality, the name of the policy is not significant as long as there is a policy that addresses viruses and other types of malicious code.

5.2.3 The level of users' knowledge of information security policies

Although technical professionals are expected to implement technical information security measures, procedures and standards are supposed to be implemented by all users in an organisation. The word 'user' in this study refers to any information systems users such as employees, independent contractors, service providers, consultants, and all personnel affiliated with third parties who are based in the relevant company. It is therefore imperative for all employees to be familiar with the information security policies and, by implication, the legal requirements. It would be a futile exercise for any organisation to have policies that are not known and complied with by the targeted information systems users.

Users have elementary knowledge of information security policies

During an interview with an online florist general manager (services sector), it was revealed that some users perceive information security policies as an irritation because they curtail their freedom to do certain things in the information systems space. This claim was supported by an online restaurant franchise webmaster (services sector) who observed that the problem is that such things have the potential of infringing on information security or violating acceptable electronic communication in the corporate environment. On the other hand, other users feel that acquainting themselves with the policies is time-consuming and interferes with the actual work. This finding was supported by the Information Security Officer of an airline company: "*I think getting employees to be conversant with information security policies is always a problem because people always feel that security policies get in their way and it's something that hinders them from doing their work. It is generally difficult to get people to pay attention to policies and all that*".

[15] Interview with the Head of Virtual Channels in a bank.

The interest and level of users' knowledge is also affected by the specific security issues: "*In our organisation it [user's knowledge levels] depends on which topics of the policy. I think there's a high degree of awareness around, for example, choosing strong passwords. You know how to use a strong password because of some awareness campaigns but also because we have mechanisms that actually force them to do that, so when they log into that domain, they have to have these eight characters, it can't contain letters of their first names, it has to have at least one numeric, lower case, and upper case, so it's forcing them to do that".*[16]

This study found that users who are employees familiarise themselves better with policies than users who are customers. This is highly prevalent in the banking environment where many Internet Banking holders have been victims of fraud despite the fact that banks have placed policies on their websites to assist the users: "*Users who are professionals in their own right would be ignorant of basic information security requirements and they lose lots of money due to this. When criminals plunder their accounts they plead ignorance and expect the bank to refund them*".[17] This study established that whilst users are knowledgeable with policy aspects such as passwords, acceptable usage of e-mail and Internet, they have only a rudimentary knowledge of information security issues such as phishing e-mails, pharming websites, and spoofing scams.

The organisation's seriousness towards its policies affects users' knowledge

Two of the organisations that participated in this study have information security policies that are not formally approved by their relevant authorities. One of the organisations is in the hotel industry and the other is an online retailer. In one of these organisations, the policies are relatively new, whilst in the other organisation, policies were introduced four years previously, but they are not yet approved. One should note that the non-approval applies to all organisational policies and not just ICT policies. Although policies have been posted on the Intranets of the aforesaid organisations, employees do not take the time to study them because they will only become effective after approval. A Supply Chain Manager in an online bookseller entity noted that: "*This is a very problematic area because these policies have not yet been formally approved. Although they are on the Intranet, I'm pretty sure that our staff doesn't read this stuff because they are not yet approved*".

[16] Interview with the Manager: Applications Architecture in an airline company.

[17] Interview with the Director of Self Service Banking.

During the interviews, the researcher learnt that the approval of policies is not an indication that the policies are accepted / implemented. Each employee has to sign that they accept each information security related policy and will adhere to it; unless the provisions of the policies were included in their employment contracts (see Appendix D for an example of Employee Interception Consent). Signing of the policies by each employee should be preceded by extensive training. Organisations can only do this if they are serious about information security. Lack of seriousness on the part of the organisation will permeate to the level of individual employees and this does not bode well for the information security endeavours in the corporate environment.

Information security policies awareness programmes are superficial

It was found that although policies could have been properly established and approved, the adherence to them is not effective because the main form of awareness training is to post policies on the Intranet. A General Manager: Networks in a hotel defended the department in relation to the superficial awareness of information security policies: "*It is not our responsibility to train employees; we're IT people. We coordinated the drafting of the policies, forwarded them to a law firm in Cape Town which specialises in IT law, and then got them approved. You are barking up the wrong tree; the culprits in this matter are the HR (Human Resources) guys. HR should do this as part of the training, induction, or orientation programmes. The sooner they spend less time training people about dressing and eating etiquette the better*". i.e. – they are playing the blame game - a clear indication that they themselves are not really embracing the policies and 'living' by them!

Even in organisations where the Human Resources Department wants to conduct awareness programmes, their efforts are usually met by stiff opposition from the 'core-business' departments which perceive an information security awareness campaign as a waste of time. The problem is that they cannot link information security and market competitiveness (billable work). This is being disingenuous because a company cannot thrive and make profits because poor information security would lead to huge financial losses and reputational damage. For example, if a bank decided to ignore information security measures, "*It would become non-existent within a week. Hackers will have easy access; depositors will march and demand their money because the institution would have suffered bad media publicity. The so-called core departments should get their act right and release their staff members for* *information security awareness programmes; stakes are very high"*.[18] This view is supported by a Director of Self Service Banking: "*Risk Management should be seen as an integral part of profit making and organisational sustainability*". Companies should learn to incorporate information security policies awareness between competing priorities, since information security cannot be compromised. Any profit generation at the expense of proper information security implementation cannot be sustained in the long term or even in the short term, depending on the nature of the organisation.

A hotel group that participated in this study appeared to be a little more serious regarding information security awareness: "*We run policy awareness. It's a two hour session and we basically preach four policies. This is complemented by an online session which is called 'O-Camp'; basically the user goes through that – it's an hour session. It's the four policies and at the end they get certification, but you have to pass. The CEO has made it clear that it is compulsory, so if you don't come for this session, we will invite you again and again, until you come"*.[19] Whilst this awareness programme is commendable, it remains artificial. After going through the interviews and collecting documents, the researcher's view is that each session of information security policy awareness should be preceded by pre-assessment to determine the level of participants' knowledge; this should be followed by post-assessment after the actual awareness session. The post-assessment activities will determine the level of new knowledge gained. This recommendation is applicable to all organisations and not just the aforementioned hotel group (see Section 8.2.4).

Users are suffering from compliance fatigue

Mentioning the word "compliance" to a group of banking, mining or insurance employees may well result in a negative response, because they are expected to comply with a myriad laws, regulations, procedures and policies. In the banking sector, executives indicated during the interviews that they are buckling under the weight of 150 non-banking laws and the requirements of Basel III regulations. Although information security is highly prioritised in the abovementioned sectors, information security awareness policies have to compete with other compliance requirements. Problems emanate when the relationship between the employer and employee deteriorates and the employee becomes an information security risk;

[18] Interview with the CEO: Mobile and Transect Solutions

[19] Interview with the Chief Information Officer.

that is why in a corporate environment most information security crimes are committed internally, sometimes with external cooperation. A bitter IT employee may deliberately destroy information systems. When the matter is taken to the South African Commission for Conciliation, Mediation and Arbitration (CCMA), the estranged employee usually pleads ignorance and the company is blamed for insufficient awareness programmes. Ordinary employees may sell information to the company's competitors. A Senior Channel Manager: Cellphone and Electronic Channels in one of the big four banks proclaimed: "*You also have users who are honest and genuine employees; their main weakness is gullibility and lack of proper training in terms of security. When such employees are confronted with a 'social engineer' they become naive and fall in the trap; this is very sad. Whilst compliance fatigue is a genuine issue, information security policies awareness should remain on our radar screen*".

Information security practitioners have to be creative to gain and keep the attention of the targeted audience. However, one should hasten to add that information security policies awareness should not be done at the expense of other compliance requirements.

5.3 SUMMARY

This chapter presented the findings of this study which were obtained through interview data collection method. It has already been mentioned in several sections of this chapter that these findings were derived from the data collected through interviews with information security practitioners and information security and legal experts. The main findings of this study reflect that the participation of some Boards of Directors in the provision of the information security policies was minimal; some information security practitioners were not familiar with the legal and policy aspects that they were supposed to be integrating into the implementation of information security and thus most organisations were not complying with the law.

Some of the laws which featured in Chapter 3 where the legal framework of this study was presented do not appear in the findings obtained from the interviews of this study. These include the following laws: the Companies Act No. 71 of 2008 and the National Credit Act No. 34 of 2005.

The researcher chose to use the term ‘genre of design’ as stated in Chapters 1 and 4, and therefore both ontology and epistemology played an important role in the findings of this study that were obtained through interviews. That is why the findings contained in this chapter are a product of interplay between the personal philosophical perspective of the researcher and the empirical findings of the study. The next chapter presents findings of this study that were obtained from document collection and websites analysis.

CHAPTER SIX
FINDINGS OF THE STUDY: FINDINGS FROM DOCUMENT COLLECTION AND ANALYSIS

6.1 INTRODUCTION

In the previous chapter, findings obtained through interviews were presented. Apart from analysing the interview data, the policies and documents collected from the 45 organisations that participated in this study were also analysed; the findings thereof are presented in this chapter. These include, but are not limited to, the following policies: Information Security, Data Privacy, Access to Information, Interception and Surveillance, Records Management, Intellectual Property, Plagiarism, ICT Acceptable Use, and Electronic Communications policies. Of the 45 organisations that participated in this study, none had a stand-alone policy on patents protection. The policies were evaluated against the requirements, as identified in the following legislation:

i. Promotion of Access to Information Act No. 2 of 2000;
ii. ECT Act, 2002;
iii. RICA Act, 2002;
iv. Intellectual Property Law Amendment Act No. 38 of 1997;
v. Copyright Act No. 98 of 1978;
vi. Merchandise Act No. 17 of 1941;
vii. Films and Publications Act No. 65 of 1996;
viii. National Archives and Records Service of South Africa Act No. 43 of 1996; and
ix. Constitution of the Republic of South Africa No. 108 of 1996.

Section 6.2 provides a discussion of the policy analysis. Other documents collected, apart from the policy documents, included those that deal with ICT processes and procedures. Through the document analysis, it was found that some organisations in South Africa were not sufficiently integrating legal and policy aspects in the implementation of information security.

Categories and sub-categories of the findings obtained through website analysis were produced after the data collection and analysis of the websites that were designed for financial transactions in the 45 organisations. Findings obtained through the analysis of websites' analysis notes indicate that the websites of some South African organisations do not comply with the requirements of the legislation. These are the websites through which financial transactions take place. Section 6.3 provides more detailed information. Table 6.1 below summarises the analysis and shows the relationship between categories and sub-categories.

Table 6.1: Summary of Analysis showing the Relationship between Categories and Sub-categories

Document collection and analysis	Policies regarding hacking	• Overview of policies • Information security policies • Interception and surveillance policies
	Policies regarding intellectual property	• Overview of policies • Plagiarism policies • Document and record management policies
	Policies regarding the protection of trademarks	• Overview of the intellectual trademark guidelines
	Policies regarding privacy	• Overview of policies • Data privacy policies • Acceptable use policy • Electronic communication policy • Policies regarding patent right
Websites analysis	Financial transaction functionality of website	• Enables consumers to make payments for products or services. • Lack of compliance may expose customers • The absence of a disclaimer as a hyperlink may expose the merchant to litigation
	A lack of familiarity with the requirements of the ECT Act No. 25 of 2002 regarding consumer protection	• The elementary nature of legal notices • Limited attempts to comply with relevant policies

In this chapter, the researcher offers his own interpretation and understanding of the data. This is accordance with the selection of the 'genre of design' as stated in Chapter 4 (section 4.1). The researcher also mentions in the Disclaimer, which appeared at the start of this thesis, the IANAL principle of, "I am not a lawyer", illuminating that this study is not a legal research but rather an information systems research.

6.2 FINDINGS OBTAINED THROUGH DOCUMENT COLLECTION AND ANALYSIS,

Information security related policies were collected from 30 of the 45 organisations that participated in this study. Other organisations could not provide the documents, either because they did not have them or there were concerns about confidentiality. The collected policies were analysed against information security-related legislation and the analysed interview content. It is important to state that only 14 of the 30 companies, whose policies were analysed, have integrated legal aspects into their policies and the provision of information security. Three of these 14 companies, that have integrated legislation in their policies, had only incorporated legislation requirements in their Records Retention Schedules; their other information security policies do not make any reference to any law. It was found that the provisions of definitions of terms in some of the policies were essential because it enables people with no IT and/or legal background to understand the content of the policy. Table 6.2 below indicates policies that were collected from various organisations.

Table 6.2: Policies collected from the organisations

Table Key:

- "Yes" means policy is available
- "No" means policy is not available
- - means the researcher could not ascertain the availability of policy

Organisation No:	Type	Access to Information Policy	Data Privacy Policy	Electronic Communications	ICT Acceptable Use	Interception and Surveillance Policy	Information Security Policy	Intellectual Property Policy	Records Management Policy
1	Banking	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
2	Banking	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
3	Banking	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
4	Banking	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
5	Banking	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
6	Telecommunications	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
7	Online Restaurant Franchise Chain	-	-	-	-	-	-	-	-
8	Flower Delivery Service	-	-	-	-	-	-	-	-

Organisation No:	**Type**	**Access to Information Policy**	**Data Privacy Policy**	**Electronic Communications**	**ICT Acceptable Use**	**Interception and Surveillance Policy**	**Information Security Policy**	**Intellectual Property Policy**	**Records Management Policy**
9	Airline	Yes	Yes	No	No	Yes	Yes	Yes	Yes
10	Airline	Yes	Yes	No	No	Yes	Yes	Yes	No
11	Airline	Yes	No	No	No	Yes	Yes	Yes	Yes
12	Airline	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
13	Airline	Yes	No	No	No	Yes	Yes	Yes	No
14	Airline	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
15	Online Shop	-	-	-	-	-	-	-	-
16	online Shop	-	-	-	-	-	-	-	-
17	Online Retailer	-	-	-	-	-	-	-	-
18	Airline	Yes	Yes	No	No	Yes	No	No	No
19	Airline	Yes	Yes	Yes	No	Yes	Yes	No	No
20	Airline	Yes	No	Yes	Yes	Yes	Yes	No	Yes
21	Bookseller	-	-	-	-	-	-	-	-
22	Online Retailer	-	-	-	-	-	-	-	-
23	Online Retailer	-	-	-	-	-	-	-	-
24	Online Retailer	-	-	-	-	-	-	-	-
25	Cinema	-	-	-	-	-	-	-	-
26	Cinema	-	-	-	-	-	-	-	-
27	Hotel	Yes	Yes	No	Yes	No	No	Yes	Yes
28	Hotel	Yes	Yes	No	No	No	Yes	Yes	Yes
29	Hotel	Yes	No	Yes	No	No	Yes	Yes	No
30	Hotel	Yes	Yes	No	Yes	No	No	Yes	Yes
31	Hotel	Yes	Yes	No	No	No	Yes	Yes	No
32	Hotel	Yes	No	Yes	No	No	No	Yes	Yes
33	Hotel	Yes	No	No	Yes	No	No	Yes	No
34	University	Yes	Yes	Yes	Yes	No	No	Yes	Yes
35	University	Yes	Yes	Yes	Yes	No	No	Yes	No
36	Hotel	-	-	-	-	-	-	-	-
37	Broadcasting	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
38	Broadcasting	Yes	Yes	Yes	No	No	No	Yes	Yes
39	Online Shop	-	-	-	-	-	-	-	-
40	Car hire	Yes	No	No	Yes	No	No	Yes	No
41	Car hire	Yes	No	No	Yes	No	No	Yes	Yes
42	Car hire	-	-	-	-	-	-	-	-
43	Telecommunications	Yes	Yes	Yes	Yes	No	No	Yes	No
44	Telecommunications	Yes	Yes	No	No	Yes	No	Yes	Yes
45	Telecommunications	Yes	Yes	No	Yes	No	No	Yes	No

It was stated in Section 6.1 that only 30 (out of 45) organisations that participated in this study provided their policies to the researcher. The researcher could not ascertain if the other 15 organisations had these policies or not. On the other hand, it is important to note that all the policies reflected in this chapter are information security policies; however, some organisations have a policy specifically named: “Information Security Policy”.

Although 13 (out of 30) organisations that provided their policies did not have a policy called “Information Security”, some of the provisions of what would be contained in this policy could be found in other policies.

Plagiarism Policy does not appear in the above table due to space constraints. Out of 30 organisations whose policies were collected by the researcher, only two universities and two broadcasting companies had plagiarism policies.

Interestingly, all the 30 organisations that provided their policies to the researcher have Access to Information Policy. In some of the organisations it is referred to as Access to Information Policy and / or Promotion of Access to Information Manual. This high compliance should be attributed to the fact that all companies in South Africa are required by the Promotion of Access to Information Act No. 2 of 2000, to have access to information related policies or manuals.

For the purpose of this study, policies have been grouped into five areas of information security: hacking, intellectual property and copyright, protection of trademarks, privacy, and patents protection. This means an organisation may not have a Data Privacy Policy, but its privacy-related matters may be catered for in the ICT Acceptable Use Policy and/or Electronic Communications Policy. Table 6.3 below provides an overview of the findings in this section.

Table 6.3: Synopsis of the document collection and analysis findings

AREA OF INFORMATION SECURITY	RELEVANT POLICY	RELEVANT LEGISLATION
1) Hacking	• Information Security Policy • Data Privacy Policy • Access to Information Policy • Interception and Surveillance Policy • Records Management Policy	• Promotion of Access to Information Act No. 2 of 2000 • Electronic Communications and Transactions Act No. 25 of 2002 • Regulation of Interception of Communications and Provision of Communication-related Act No. 70 of 2002
2) Intellectual Property and Copyright	• Intellectual Property Policy • Information Security Policy • Data Privacy Policy • Plagiarism Policy • Records Management Policy	• Intellectual Property Law Amendment Act No. 38 of 1997 • Copyright Act No. 98 of 1978 • Merchandise Act No. 17 of 1941 • Films and Publications Act No. 65 of 1996 • National Archives and Records Service of South Africa Act No. 43 of 1996
3) Protection of trademarks	• Intellectual Property Policy	• Intellectual Property Law Amendment Act No. 38 of 1997 • Copyright Act No. 98 of 1978 • Merchandise Act No. 17 of 1941
4) Privacy	• Data Privacy Policy • ICT Acceptable Use Policy • Electronic Communications Policy • Interception and Surveillance Policy	• Constitution of the Republic of South Africa No. 108 of 1996
5) Patents protection	• No company had a clearly distinguished policy on patents rights	• Patents Act No. 57 of 1978 • Notes: Only three organisations addressed the patents protection as part of the Intellectual Property Policy

In comparing Table 6.3 above with Table 7.1 in Chapter 7, it will be noted that although none of the policy documents collected from the participants in the study link the ECT Act (2002) to copyright-related policy issues, Chapter XI of the aforesaid Act contains some copyright related issues (see Table 6.1). Detailed findings of the document analysis are presented below.

Hacking has much to do with access control. Hacking was found to be addressed in several policies, including the Information Security Policy and Interception and Surveillance Policy. The relevant pieces of legislation are the Promotion of Access to Information Act, the ECT Act and the Interception Act. An overview of the policies relevant to hacking has been provided in the following paragraphs. This overview presents a snapshot of the information security policies and interception and surveillance policies collected from some of the companies that participated in this study. The overview is biased towards the aspects that contain legal provisions.

6.2.1 Policies regarding hacking

This study found that although policies such as Data Privacy, Access to Information, and Records Management tentavely address issues related to hacking policies that are more applicable to hacking are Information Security, and Interception and Surveillance. Information Security and Interception and Surveillance policies are discussed in more detail below.

Brief overview of information security policy

Some of the policies provided definitions of the terms used in the policies. Most of these terms are information security terminologies such as ‘access control, audit logs, authentication, centralised data, consumer, corporate data, decentralised data, dual control, encryption, equipment, error log, firewalls, information asset, information security officer, operating systems, service level agreement, transaction, users, user requirement specification, and viruses. The provision of definitions is an essential step towards enhancement of information security in the corporate environment as it enables non-IT users to understand the policies with ease.

Relevant legislation, policies, and other documents

In this section, it is stated that ICT makes the organisation vulnerable to some legal risks and liabilities in a number of ways. The information security policy details rules, guidelines and standards to ensure the security of the organisation’s information, data, records and documents. This policy applies to all users using digital processing and communication equipment/infrastructure, including third parties that have temporary access to and/or use of the organisation’s communication facilities or equipment to create, access or use the organisation’s information.

The relevant legislation in respect of the Information Security Policy is as follows:

- Promotion of Access to Information Act No. 2 of 2000;
- ECT Act, 2002; and
- RICA, 2002.

The policy provides appropriate coverage of International Standards ISO 27002. The Information Security Policy should be read in conjunction with the following policies: ICT Acceptable Use Policy; Data Privacy Policy; Access to Information Policy; Interception and Surveillance Policy; and Records Management Policy.

Overview of the Interception and Surveillance Policies

Some of the interception and surveillance policies contained definitions of the terms used in the policies. These include the following terms: authorised persons, communication facilities, employees, intercept, Internet, monitor, and personal information.

Relevant legislation, policies, and other documents

It was interesting to learn that in two of the collected policies, it was stated from the onset, that the Interception and Surveillance Policy emanates from the Constitution of the Republic of South Africa No. 108 of 1996, which places the emphasis on privacy and dignity. Whilst most of the information security-related policies are silent on the rights of the employees, in this particular policy there are provisions such as: "This organisation is committed to the provisions of the South African Constitution and the protection of employees' privacy and dignity". This policy aims to balance the privacy and rights of employees with the security and risk management obligations of the organisation by providing strict rules and limitations to the interception and monitoring of communications.

In all the policies that the researcher collected, it was clearly stated that, in terms of the scope of application, the policy applied to all employees and any service provider employed to assist the organisation in the monitoring and surveillance of employees' conduct and communications. The relevant legislation for this policy is the Constitution of the Republic of South Africa No. 108 of 1996; RICA, 2002; ECT Act, 2002; and the Guidelines of the National Archives. A careful scrutiny of the collected policies showed that most clauses of the interception and surveillance policies refer largely to the RICA, 2002. It is also stated that this policy should be read in conjunction with the Data Privacy Policy.

6.2.2 Policies regarding intellectual property and copyright

After studying the collected documents from the organisations that participated in this study, the researcher found that there is little differentiation between the concepts of intellectual property, copyright and trademarks. In effect, organisations use these words synonymously and interchangeably. However, this does not have any impact in terms of the quality of the intellectual property, copyright, and trademarks policies and their implementation. Whilst most of the information security policies have been marked "Internal Only", policies and guidelines are placed on the organisation's website. Table 6.1 illustrated the relationship between the main-category and sub-categories pertaining to the findings regarding intellectual property and copyright that were obtained through document collection and analysis.

As explained previously in Chapter 3, the inception of ICT, and the Internet specifically, has led to a copyright challenge. Intellectual property and copyright is addressed in several policies, including the following: Intellectual Property Policy, Information Security Policy, Data Privacy Policy, Plagiarism Policy, and Records Management Policy. The relevant legislation includes the Intellectual Property Law Amendment Act No. 38 of 1997; the Copyright Act No. 98 of 1978; the Merchandise Act No. 17 of 1941; the Films and Publications Act No. 65 of 1996; and the National Archives and Records Service of South Africa Act No. 43 of 1996. An overview of the policies relevant to Intellectual Property and Copyright are provided below. The overview presents the policies collected by the researcher from some of the companies that participated in this study. The overview is biased towards the aspects that contain legal provisions.

Brief overview of the intellectual property and copyright policies

Intellectual Property is gradually becoming an important asset amongst South African companies. According to the information contained in the collected policies, it includes assets such as, but not limited to, 'website content, website source code, software developed within a particular company, software developed by employees, product packaging, trademarks, domain names, marketing information, and the like. Copyright is addressed by the Intellectual Property Policy. A few of the collected intellectual property and copyright policies include the definitions of terms, such as content providers, employees, external ICT IP (Intellectual Property), ICT IP, and responsible person.

Relevant legislation, policies, and other documents

The objective of this policy is to formulate a framework for the establishment, protection, registration, maintenance, management and use of ICT Intellectual Property. This policy is applicable to all employees, third parties, external contractors, and ICT Intellectual Property-related contracts entered into by employees acting on behalf of the organisation. The relevant legislation includes the Intellectual Property Law Amendment Act No. 38 of 1997; the Copyright Act No. 98 of 1978; and the Merchandise Marks Act No. 17 of 1941. The problem is that some of the aforementioned laws are very old and were introduced before the Internet was used for commercial purposes. Other relevant policies for intellectual property, copyright and trademarks are the Information Security Policy and the Data Privacy Policy. It is a matter of extreme concern to note that the majority of the organisations that participated in this study do not have policies that adequately address the protection of intellectual property, copyright and trademarks.

Some of the copyright provisions placed on the websites of organisations that participated in this study contain the following paraphrased stipulations:

Organisation "38" respects the intellectual property of other organisations, and thus we expect our competitors, users of our products and websites to do the same. Organisation 38 may, in proper circumstances and at its discretion, cancel the access of users who violate the intellectual property rights of our company. We encourage you to exercise discretion while browsing our website. The use of original texts, graphics, images, screen shots, and other materials from Organisation 38 sources must be approved by Organisation 38. In addition, when using such materials, you must include a copyright notice – in an adjacent area or as a footnote – to show Organisation 38 copyright. Please note that Organisation 38 photography is only licensed for Organisation 38 use and must not be used by other organisations in their communications.

The above paragraph was extracted from an Intellectual Property and Copyright Policy of a South African based company which operates globally. That is why the policy does not necessarily make reference to the law of any specific country. Be that as it may, Lawyer F who was interviewed during the course of this study, indicated that the aforesaid policy is within the parameters of the South African and international legal framework. The next section deals with trademarks-related policies.

The preamble of one of the two universities that participated in this study was considered to be of importance in the area of the protection of intellectual property: *The University recognises that it is a society of scholars. The University is devoted to providing a platform that supports the research and teaching activities of all its staff and students in the quest for excellence and for the public good. The University wishes to encourage all members of its community to produce original works of authorship and to engage in free expression and exchange of ideas and to let them be compensated for their knowledge and originality. This Intellectual Property and Copyright Policy has been prepared in this spirit and for this intent and to protect the intellectual property rights of the University and all members of its community.*

The two universities that participated in this study also have dedicated policies on plagiarism. These differentiate them from the other 43 organisations that participated in this study. A brief summary of plagiarism policies appears below.

Plagiarism Policy

The plagiarism policies have been approved by the Senates' committees and Councils, and are applicable to all members of the university community – students, employees, employees visiting other institutions, independent contractors, other persons engaged under contracts of service by the university, visiting lecturers, and honorary, clinical, and other members of staff not in receipt of remuneration from the university.

Effectively the plagiarism policies attempt to deal with the following broad questions and issues:

- What is plagiarism and how is it different from copying/cheating?
- How should the university deal with plagiarism? Should it be dealt with as an offence or a developmental issue or a mixture of these?
- What approach should be employed for managing plagiarism at the university?

The researcher observed that the plagiarism policies in the universities that participated in this study do not make reference to any particular law. Appendix E provides an example of possible wording of a declaration by authors. The researcher has noted that whilst some companies in South Africa are attempting to address issues around intellectual property and copyright of their logos and trademarks, it appears they have no interest in plagiarism and that is why the plagiarism policy will mainly be found in higher learning and research institutes. Other policies that were studied as part of this study are related to trademarks and are addressed below.

Records Management Policies

Regarding the rationale and scope of application, it is accepted that strong records management is fundamental to good governance and efficient business management. The researcher found that only some organisations in South Africa were ensuring that processes and procedures were in place for the proper creation, maintenance, use, and disposal of records throughout their lifecycle to achieve efficient, transparent and accountable governance. Further to the above, organisations should implement document and records management to enable the organisation to protect its intellectual property from theft, unauthorised use and destruction; support the business, legal, and accountability requirements of the organisation; support continuity in the event of fire or other disaster; comply with the records retention responsibilities specified in South African legislation; ensure the safeguarding of evidence for possible future legal action, mediation or disciplinary hearings; and processing public requests for information as outlined in the Promotion of Access to Information Act No. 2 of 2000.

The Records Management Policies impact on all personnel who create paper-based and electronic documents and records; have access to records; have any other responsibility for personnel engaged in any of these activities; or manage, or have design input into IT infrastructure.

Relevant legislation, policies, and other documents

By managing their electronic and paper-based records effectively and efficiently, certain organisations in South Africa are striving to give effect to the accountability, transparency, and service delivery values contained in the legal framework established by, *inter ali*a, the Constitution of the Republic of South Africa No. 108 of 1996; National Archives and Records Service of South Africa Act No. 43 of 1996 (as amended); National Archives and Records Service of South Africa Regulations of 1997; the Promotion of Access to Information Act No. 2 of 2000; the Promotion of Administrative Justice Act No. 3 of 2000; and the ECT Act, 2002. Further to the above, certain organisations endeavour to comply with the Records

Retention requirement as contained in their Records Retention Schedules. It is significant to note that the most important role of the Records Management Policy in most organisations which have this policy is to ensure that the intellectual property of the organisation is secured.

The protection of trademarks is mainly addressed in one policy called the Intellectual Property Policy. The relevant legislation is the Intellectual Property Law Amendment Act No. 38 of 1997, the Copyright Act No. 98 of 1978, and the Merchandise Act No. 17 of 1941. An overview of the policies relevant to trademarks has been provided below. This provided a snapshot of the trademarks related policies collected from some of the companies that participated in this study. The overview is biased towards the aspects that contain legal provisions.

Brief overview of the intellectual trademarks protection guidelines

Trademarks guidelines:

Trademarks have been catered for in the Intellectual Property Policy and thus this section will not pay much attention to this policy. The purpose of this policy in relation to trademarks is to create a framework for the creation, protection, registration, maintenance, management and exploitation of the organisation's trademarks. Over and above the Intellectual Property Policy, organisations in South Africa have developed guidelines for the use of their trademarks. Other than ensuring that their trademarks should not be stolen, some of the organisations have gone to great lengths to ensure that even people who have permission to use their logos should ensure that the quality of the logos is not compromised. Some of the organisations have produced booklets or technical guides on the usage of their corporate identities. The booklets are intended to set minimum standards to ensure consistency throughout a particular company. Guidelines in the booklets deal with issues such as colour usage and logo usage. Table 6.4 below provides an example of such logo usage guidelines.

Table 6.4: Guidelines for corporate logo usage

GUIDELINES ON COLOUR USAGE	GUIDELINES ON LOGO USAGE
• When printing in matt • When printing in gloss • Text colour matt or gloss • When using a colour background	• Do not alternate colours within the logo • Do not alter proportions of logo or text • Always try and print half tone • Wherever possible, print the logo in full colour. If you need to use the logo in 2 colours, follow the guide in the booklet. • Do not use a different form or split the company name. • Do not remove the by-line.

Whilst issues related to the usage of the logo may appear to be irrelevant, it is the view of the researcher that they are an essential part of information security since fraudsters use trademarks to deceive the potential victims. A Chief Information Officer whose airline company participated in this study, concurred with this claim. Applicable legislation in this area includes the Intellectual Property Law Amendment Act No. 38 of 1997; the Copyright Act No. 98 of 1978; and the Merchandise Act No. 17 of 1941. The next sub-section will deal with policies regarding privacy.

6.2.3 Policies regarding privacy

Table 6.1 illustrated the relationship between the main-category and sub-categories pertaining to the findings regarding privacy that were yielded through document collection and analysis. This study has found that privacy as an information security issue has been addressed in many policies, including for example the Data Privacy Policy, the ICT Acceptable Use Policy, the Electronic Communications Policy, and the Interception and Surveillance Policy. These policies are mainly based on the Constitution of the Republic of South Africa No. 108 of 1996. An overview of the policies relevant to privacy is provided below.

Brief overview of the privacy policies

Privacy is largely catered for in various information security-related policies such as Data Privacy Policy, ICT Acceptable Use Policy, and Electronic Communication Policy.

Data Privacy Policy

Rationale and scope of application:

The organisation may be liable for the unauthorised use of personal information of employees, suppliers, consumers, and other third parties. In terms of Section 14 of the Constitution of the Republic of South Africa No. 108 of 1996, everyone has the right to privacy. This right extends to the commercial domain and employees and others continue to enjoy the protection of their privacy even when they enter the workplace or take part in commercial activities. Two of the Data Privacy Policies perused by the researcher went to the extent of referring to court cases and summarised the privacy right as follows: ‘an individual has the right to decide when, how and under which circumstances, personal facts of that individual may be disclosed. This policy applies to all users as well as third parties that have temporary access to the organisation's records, documents, agreements, e-mail, internet access or IT network. The terms defined in the policy include information, privacy subjects, and users.'

Relevant legislation, policies, and other documents

With regard to legislation, the policy refers to the Constitution of the Republic of South Africa No. 108 of 1996. The policy should be read in conjunction with other policies such as the ICT Acceptable Use Policy; the Electronic Communication Policy; and the Interception and Surveillance Policy. After studying the Data Privacy Policies, the researcher concluded that there is information that the employer deems highly sensitive and information that the organisation may deem necessary to gather – sometimes without even necessarily gaining the consent of the employees/users of the information systems. This has been catered for in the policy by a clause that allows an organisation to have access to, or to collect, certain information from the users. Table 6.5 below distinguishes information that requires user consent and information that may be collected without user consent. This distinction was obtained from the fieldwork.

Table 6.5: The collection of information with or without consent

INFORMATION TO BE COLLECTED WITH USER CONSENT	INFORMATION COLLECTED WITHOUT USER CONSENT
• Information relating to the race, gender, sex, pregnancy, marital status, nationality, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language, and birth of the individual; • Information relating to the education or medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved; • The address, fingerprints or blood type of the individual; and • Correspondence sent by the individual that is implicitly or explicitly of a private nature or further correspondence that would reveal the contents of the original correspondence.	• IP Addresses: The organisation will use the IP addresses to help diagnose problems, to administer the web site, the system administrator will only recognise the user domain name and not the user e-mails; • The organisation may use cookies to deliver personalised content, to save the user from having to re-enter his/her email address repeatedly, to keep track of the shopping cart, and to tailor the information offerings to how users use the site; and • Personal information may be collected for non-personal statistical purposes.

An online retail based ICT Operations Manager interviewed in this study argued that the collection of any personal information without individual consent – especially in the working environment – may be illegal and a violation of the RICA Act, 2002. The Employer may therefore have to request the employees to sign a detailed Employee Interception Consent (see

Appendix D for an Example of an Employee Interception Consent). If the employee refuses to sign the consent or agree to the policy, the provisions of the labour law (Labour Relations Act No. 66 of 1995) and policies will become applicable.

Acceptable Use Policy

Rationale and scope of application:

The organisation's intention for establishing an Acceptable Use Policy is not to enforce restrictions that are imposed contrary to the organisation's conventional culture of openness, trust and integrity. The introduction of the policy shows the commitment of the organisation to protect its employees, partners and the organisation from illegal or damaging actions by any person. This policy applies to employees and third parties who use and have access to the information systems. The policy also applies to all equipment/infrastructure that is owned, rented or leased by the organisation.

The purpose of the Acceptable Use Policy is to outline the acceptable use of ICT equipment/infrastructure at the organisation. The policy also makes provisions that prevent the use of ICT equipment to infringe the privacy of the users and employees. Inappropriate use of the ICT equipment exposes users' privacy to violation and the organisation to risks including viruses, compromise of network systems and services, intellectual property and legal challenges. The Acceptable Use Policy usually defines terms such as communication facilities, equipment, illegal content, intercept, offensiveness, privacy, personal information, pornography, spam, and users.

Relevant legislation, policies, and other documents:

The Acceptable Use Policies draw their mandate and legal framework from the following laws – the Promotion of Access to Information Act No. 25 of 2000; the Films and Publications Act No. 65 of 1996; and the ECT Act, 2002. These Acts are mentioned in the policies that deal with acceptable use. The policy should be read in conjunction with the Data Privacy and Electronic Communications Policies.

Electronic Communications Policy

Rationale and scope of application:

The purpose of the Electronic Communications Policy is to ensure that the organisation has the legal right to: secure and maintain its computer network, equipment and communication facilities; ensure the confidentiality of its trade secrets, client information, employee information, and confidential information generally; protect the privacy of its clients; identify and address the potential risks associated with the use of technology and communication facilities in the workplace; promote employee productivity; comply with the provisions of laws and regulations that govern the access, use and interception of communications; investigate and prosecute illegal or unauthorised use of its communication facilities and/or equipment; and respect and protect every employee's right to privacy, free speech and the right to receive and impart with information as detailed, amongst others, in the South African Constitution of 1996. There is much emphasis regarding the adherence to the law and the respect of privacy. The researcher took note of the reference to the Constitution of the Republic of South Africa in some of the electronic communications-related policies; this is highly commendable, since the essence of this study is to investigate how corporate South Africa is complying with information security legislation and to propose a model that will enhance compliance.

In Organisation 18, legal briefs and privacy-related cases were attached to the policy. This would allow users to have a broader view regarding privacy-related matters. The scope of the Electronic Communications Policies applies to all users as well as to third parties that have temporary access to, and/or use of the organisation facilities or equipment. Some of the policies contained definitions of the terms: discriminatory content, illegal content, intercept, and pornography.

Relevant legislation, policies, and other documents:

The Electronic Communications Policies are written within the parameters of the following pieces of legislation: the Promotion of Access to Information Act No. 2 of 2000; the Films and Publications Act No. 65 of 1996; and the ECT Act, 2002. Some of the collected policies also made reference to the Constitution of the Republic of South Africa No. 108 of 1996. These Acts are mentioned in the policies that deal with electronic communications. The

Electronic Communications Policies should be read in conjunction with the Data Privacy and ICT Acceptable Use Polices.

6.2.4 Policies regarding patents rights

None of the companies that participated in this study had a separate policy on patents. Only three organisations addressed patent protection as part of their intellectual property policy. The researcher concluded that this could be due to the fact that most companies that participated in this study perceive the South African patent laws to be ineffective. According to the Patents Act No. 57 of 1978, computer programmes cannot be patented; however, companies are patenting these programmes regardless of the Act, in other words, CIPC (Companies and Intellectual Property Commission), an organ of the state responsible for patents registration, does not itself respect the Act governing patents. The next section contains findings obtained through the analysis of websites functionality and content.

6.3 FINDINGS OBTAINED THROUGH WEBSITE FUNCTIONALITY AND CONTENT ANALYSIS IN THE STUDY

The researcher investigated the websites of the 45 organisations that participated in this study. The purpose of the website functionality and content analysis was to determine if the websites enable financial transactions and if they do, whether they complied with the following information security legal requirements: availability of a legal notice; terms and conditions available as hyperlinks; liability disclaimers available as hyperlinks; compliance with the provisions of Chapter 3, Part II and Chapter 7 of the ECT ACT, 2002; positioning and correct implementation legal notices; availability of a legal notice that is printable or saveable as required by section 11(3) of the abovementioned Act; and availability of policies that address legal compliance of websites. Table 6.6 below reflects the findings of the website analysis.

Table 6.6: Number of organizations compliant with the legislation governing websites and e-commerce

NO.	ASPECT ANALYSED	NUMBER OF ORGANISATIONS
1.	Websites with legal notices at all	29
2.	Websites with terms and conditions available as hyperlinks	18
3.	Websites with liability disclaimers available as hyperlinks	16
4.	Websites with legal notices that address the provisions of Chapter 3, Part II and Chapter 7 of the Electronic Communications and Transactions Act	12
5.	Websites that position and implement legal notices correctly	9
6.	Websites legal notices that are printable or saveable as required by Section 11(3) of the Electronic Communications and Transactions Act	7
7.	Organizations that have policies that address websites' legal compliance	13

6.3.1 Financial transaction functionality of website

The websites of all the organisations that were analysed had useful financial transaction functionality which enables consumers to make payments for the products or services using credit cards online. From Table 6.6 above, one deduces that some companies in South Africa are not complying with the legal requirements for websites. This may expose the consumers to cyber-crime during electronic transactions. In the absence of legal notices, terms and conditions and legal policies that address compliance, consumers will have very little recourse if they are defrauded or if their privacy is violated by using a website of a particular organisation to conduct financial transactions. On the other hand, the absence of a disclaimer as a hyperlink on the website may expose the merchant to litigation.

6.3.2 A lack of familiarity with the requirements of the ECT Act No. 25 of 2002 regarding consumer protection

It appears that most IT and information security practitioners are not familiar with the requirements of the ECT Act, 2002 regarding consumer protection. Although 29 out of 45 websites that were analysed have legal notices, these are elementary in nature. These legal notices, and/or 'terms and conditions' do not make provision for all or some of the following legal requirements: definitions and interpretation, allowed usage and license, intellectual property rights and domain name use, software and equipment, disclosures required by Section 43 of the ECT Act, 2002; changes and amendments, privacy, hyperlinks to third parties, security, disclaimer and limitation of liability, removal and correction of content, interception of communications, entire agreement and severability, agreement required in terms of Section 21 of the abovementioned Act, applicable and governing law, and legal costs. Table 6.6 indicated limited and partial compliance. In the case of some websites, there is no attempt to comply with relevant policies at all.

6.4 SUMMARY

This chapter presented the findings of the study that were derived from documents collection and analysis, and website analysis.

Some of the laws which featured in Chapter 3, where the legal framework of this study was presented, do not appear in the findings of the fieldwork of this study. These include the following laws: the Companies Act No. 71 of 2008 and the National Credit Act No. 34 of 2005. On the other hand, some of the laws that were not interrogated in Chapter 3, emerged from the findings of this study; these include the Merchandise Act No. 17 of 1941, the Films and Publications Act No. 65 of 1996.

The researcher chose to use the term ‘genre of design’ as stated in Chapters 1 and 4, and therefore both ontology and epistemology played an important role in the findings presented in this chapter. The findings contained in this chapter are the results of the interchange between the personal philosophical outlook of the researcher and the fieldwork findings of the research. The next chapter presents the contribution of the study to the existing body of knowledge regarding information security.

CHAPTER SEVEN
CONCEPT MODEL OF LEGAL COMPLIANCE FOR INFORMATION SECURITY IN THE CORPORATE ENVIRONMENT

7.1 INTRODUCTION

The previous chapters, through the literature review and the findings of the fieldwork, depicted the operational necessity and legislation requirements for the integration of legal aspects into the implementation of information security. As articulated in the first chapter, it was found that no concept model exists to guide corporate South Africa in implementing information security within the broader framework of the law. This chapter will, by proposing a concept model, synthesise legal requirements and operational information security necessities into a single model. This chapter thus embodies the contribution of this study to the body of information security theory and knowledge.

This chapter suggests a model whereby legal requirements are incorporated into the information security endeavours – policy formulation, implementation, monitoring, and evaluation. This model is the intellectual property of the writer and can be viewed as a synthesis of theory, practice and cognitive perspectives gained over years of studying and practical experience. The model was necessitated by the findings of this study which reveal that both the government and corporate South Africa were not implementing some of the legal information security provisions. This model will be useful to policy formulators, directors of boards, ICT executives, and information security practitioners.

In order to demonstrate how the proposed model can be implemented in a corporate environment, a hypothetical company (Aifheli (Pty) Ltd) in which the model would be implemented was constructed. Consequently, aspects related to the model are genuine whilst the descriptions of the phantom company are fictitious, but of significance for illustration purposes. So as to illustrate how the concept model can be implemented, the study has dealt with both macro and micro aspects of the organisational implementation of the Concept Model of Legal Compliance for Information Security in the Corporate Environment. The macro organisational initiatives provide the foundation for the actual implementation of the concept model. These include the establishment and implementation of the ICT Enterprise Architecture and the implementation of the ICT governance structures. At micro level, the study demonstrates components of the concept model and the standard roles played by, amongst others, the Board of Directors, Group ICT Steering Committee, Group ICT Management Committee, Board of Directors' Audit Committee and all employees in the formulation, implementation, monitoring and evaluation of information security policies. The proposed concept model will present a structured organization that is generic in its disposition, is product-independent and will cater for both sides of information security practice, namely governance and operations.

7.2 AIFHELI GROUP OF COMPANIES

The hypothetical/phantom company is fictitiously named Aifheli Group of Companies Limited (hereafter referred to as Aifheli or the Group). Names of the people that appear in this section are also fictitious and any similarities to any real person are accidental.

Aifheli was started in 1996 by a prominent politician, Duvhalashu Tshifularo (43 years old) in South Africa. Tshifularo graduated with a BSc Computer Science degree from Reading University in the United Kingdom, and completed the Programme for Leadership Development from Harvard Business School in the United States of America. Prior to establishing this company, Tshifularo was a member of the national parliament and held the position of Chief Whip of one of the leading political parties in South Africa. He took advantage of the dawn of the new democratic dispensation and Black Economic Empowerment in South Africa and started a company. The establishment of his company was not his first experience of the corporate sector. Before 1994, he completed fellowships at the International Monetary Fund and the World Bank. He also worked in a renowned technical services company which dealt with technical inspection services, technical staffing services, consulting and training as well as management system certification.

When one of the platinum mining companies sold some of its mines, through his political connections, Tshifularo was able to raise money to buy them. Seeing that he was not a miner, he recruited a very experienced mining operator who had 25 years practical experience in the mining sector, Pieter van Tonder. Although most of these mines were almost depleted, Van Tonder used advanced technology to extract large amount of value from them. By 2002, Aifheli Mines was the third biggest platinum company in South Africa. By 2007, Tshifularo had become the first black dollar billionaire. He used the profit generated to buy other business ventures, especially those that were sold by the government as part of privatising and unbundling of State Owned Entities (SOEs). Other than mining, Tshifularo added SHERQ (Quality, Safety, Health, and Environment), ICT and HRD (Human Resources Development) to his business portfolio and expanded the Group. Aifheli was listed on the Johannesburg Securities Exchange in February 2008, followed by a secondary listing on the Botswana Stock Exchange where it had obtained some mining rights, after entering into a joint venture with a local businessman from a prominent royal family.

The Group has four entities (companies): Aifheli Mines, Aifheli SHERQ Solutions, Aifheli HRD Services, and Aifheli Autocatalytic Converter Solutions. Figure 7.1 below illustrates the structure of the Group.

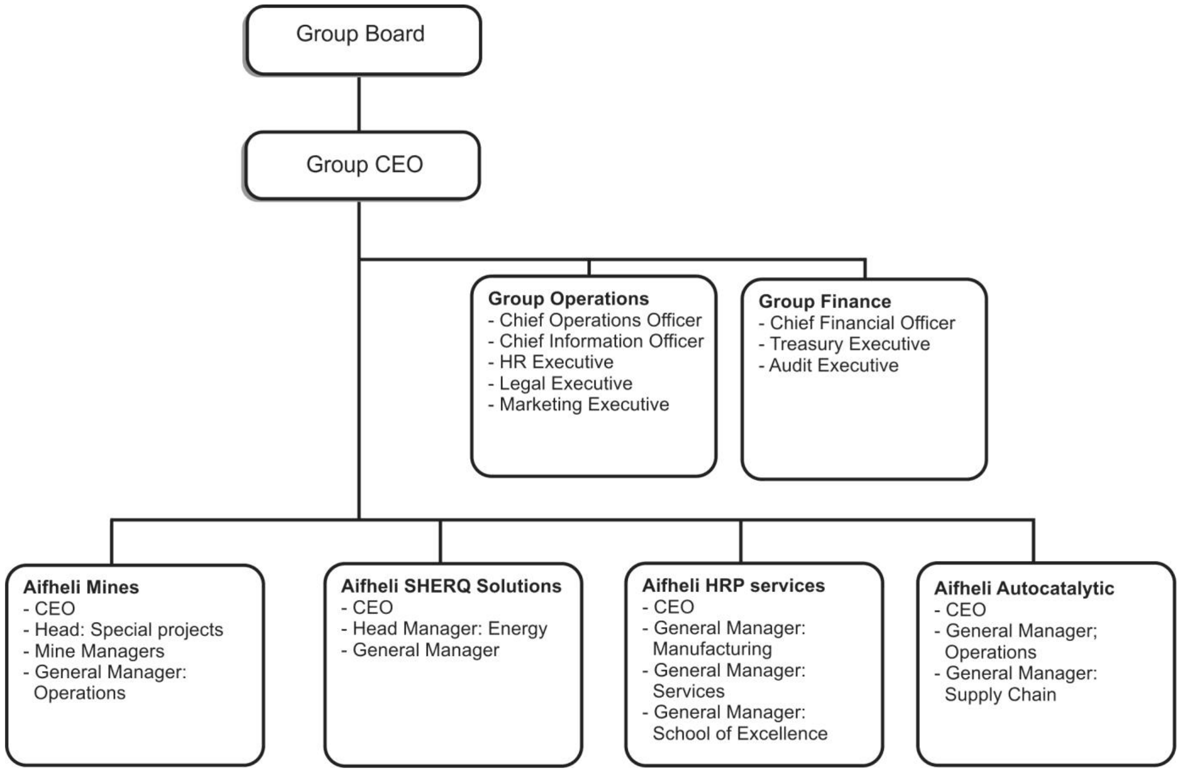


Figure 7.1: Diagrammatical representation of the structures of Aifheli Group of companies (Source: Own

Each of the Aifheli Group entities is autonomous in the running of their core operations, but at the same time they are dependent on the Group with regard to shared services.

The core business, where innovation and service production occurs, are mining, SHERQ, HRD, and manufacturing. Each core business is housed within an autonomous company (business entity) which has its own Chief Executive Officer and Executive Committee. However, the support (shared) services are managed centrally to save costs by eliminating unnecessary duplication. These support services include ICT, human resources, marketing, finance, procurement, treasury, legal affairs and auditing. For the purposes of this study, the presentation henceforth is confined to the ICT shared service, and specifically the relationship between corporate governance and information security.

7.3 THE PROPOSED MODEL OF LEGAL COMPLIANCE

This section comprises the macro and micro organisational implementation of the Concept Model of Legal Compliance for Information Security in the corporate environment. A major difference between macro and micro model implementation is that the macro level deals with overall ICT governance issues whilst at the micro level the focus is specifically on the integration of legal aspects in information security policies and the actual implementation thereof.

7.3.1 Macro-organisational model implementation

The proposed model cannot be implemented in a vacuum and thus certain ICT macro-organisational initiatives have to be in place before the actual implementation. The aforesaid macro-organisational issues include establishment and implementation of the ICT Enterprise Architecture; and implementation of the ICT governance structures.

Establishment and implementation of the ICT Enterprise Architecture

A major concern emerging from the international environment, and South Africa in particular, is that Information and Communications Technology (ICT) has, in a number of different ways, become disconnected from the business and is thus losing touch with the core activities (Bakker, 2007; Bellovin, 2013). While this can be attributed to various reasons, the major causal factor is that when major institutions evolve and restructure, they tend to temporarily lose focus. This may result in support functions like ICT assuming a corporate life of their own without necessarily being aligned to the core business of the organisation. The disconnection between ICT and the business can be resolved by establishing an Enterprise Architecture as part of implementing the proposed Concept Model of Legal Compliance for Information Security within the Group. It is thus recommended that Aifheli should establish an ICT Enterprise Architecture.

The ICT Enterprise Architecture will provide an organisational model for the deployment of ICT within the company. This ICT Enterprise Architecture, which should be aligned to the company strategy, articulates the required ICT infrastructure and its role in business processes. ICT, in this instance, should not just be seen as a support function, but should play a major role in the core business of the organisation. The suggested Enterprise Architecture should, firstly, be positioned and aligned to the four fundamental characteristics of the Aifheli core business (business reality), namely mining, SHERQ, HRD, and autocatalytic converter manufacturing. Secondly, it should cater for operational effectiveness by defining the role of ICT in the Group shared services that includes human resources, marketing, finance, procurement, treasury, legal affairs and auditing; and thirdly, there should be alignment with the governing aspects that are contained in the organisational vision, mission and strategy.

The ICT Enterprise Architecture should also be aligned to the ICT's own vision, mission, ethos and the unique operational aspects of the four entities that constitute the Aifheli Group of Companies. The ICT Enterprise Architecture should depart from the notion that "business dictates". Based on this, the ICT Enterprise Architecture should recognise the crucial role of the ICT user in the various entities within the Group in the implementation and overall management of the ICT infrastructure and applications, including information security. Critical operational expertise originates from the business entities and that is why entities within the Aifheli Group should be considered as the key drivers for ICT deployment and management. The Group ICT Department should have Service Level Agreements with each of the four Aifheli entities and the shared services. The mutually agreed business rules will strengthen the ICT Department's understanding of the business and view this as a starting point for the implementation and testing of the ICT systems. These should include the establishment and piloting of information security policies. Through the accepted business rules, the systems users understand how operational and business imperatives have been translated into platforms and processes without being concerned about the technical aspects of ICT. This principle is also applicable to the information security policies. Users should be able to comply with the legal aspects that are integrated into the policies without being legal experts.

It was stated above that ICT should play a role in the core business of the company. In other words, ICT should also be concerned about the sustainability of the organisation. In reality, ICT can contribute significantly to either the sustainability of the enterprise or the demise of the company. The ICT Enterprise Architecture should affirm the ICT mandate in terms of contributing to the balance sheet of the company. The Aifheli Group ICT Department should not merely be held accountable for embarking on activities that are not correctly aligned to the company strategy. However, ICT should be held accountable in respect of the extent of its contribution to the core business of the company. The Enterprise Architecture should give expression to the ICT mandate generally and the role of information security in the sustainability of the company. Aifheli Group ICT Department can play a meaningful role in the core business of the company if it strives to deliver service excellence and operational integrity. The ICT Enterprise Architecture should articulate how the performance of ICT as a service will be measured. Amongst others, ICT service excellence and operational integrity can be achieved by ensuring that:

- there are Service Level Agreements with the suppliers;
- a documented Group ICT Department structure exists;
- an ICT strategy is established and implemented;
- formal documented change control policy exists;
- ICT staff duties and processes are clarified and documented;
- the user provisioning processes are established and implemented;
- there are audit trails in the system;
- the Disaster Recovery Plan is established and implemented; as well as
- the establishment and implementation of the ICT policies.

Information security policies that are integrated with legal aspects will be crucial in promoting service excellence and operational integrity in the ICT Department. The provision of ICT should be aligned to national and international best practices. The Enterprise Architecture should be established within the parameters of the best-of-breed national and international standards.

Establishment and implementation of the ICT governance structures

As part of implementing the proposed Concept Model of Legal Compliance for Information Security in the corporate environment, it is suggested that the Aifheli Group should, at the macro-level, have a five-tier ICT governance structure. Figure 7.2 below illustrates the components of the ICT governance structure. This ICT governance structure should include the Board of Directors and its independent Audit Committee, Group ICT Steering Committee, Group ICT Operations Committee, ICT Entity Committees, and the Group ICT Management Committee. As indicated in the diagrammatical illustration in Figure 7.2 below, issues can emanate either top-down or bottom up.

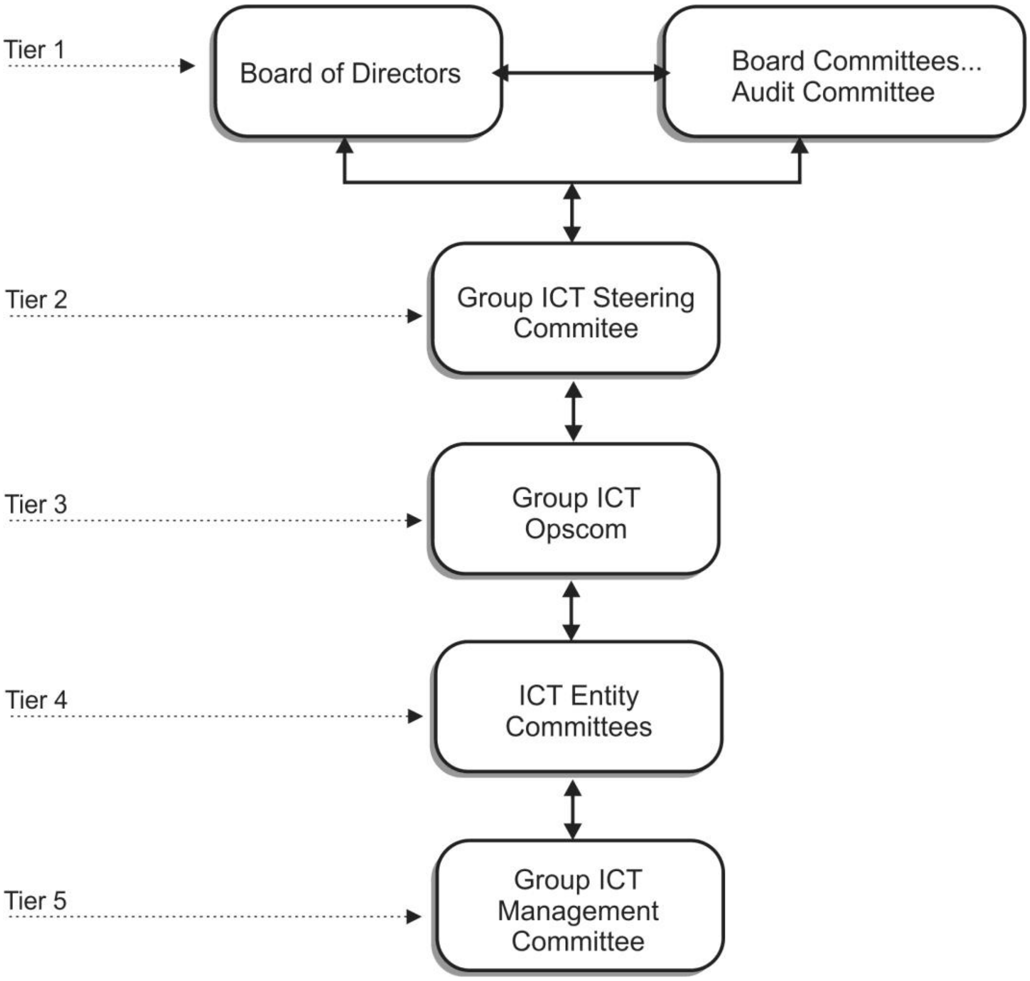


Figure 7.2: Diagrammatical representation of the ICT governance structures (Source: Own)

Tier 1: Board of Directors

The Board of Directors is the highest level of governance in any company. The Board also has fiduciary responsibilities. Between the shareholder's Annual General Meetings (AGMs) of any organisation (Non-Profit Companies, Profit Companies and Private Companies) the Board of Directors is the uppermost governance structure. This arrangement conforms to the provisions of the Companies Act No. 71 of 2008 and the King III Report (2009). According to the Companies Act, the duties of directors cater for both fiduciary responsibility and the duty of reasonable care. The implication of this is that the business and activities of an organisation should be conducted under the management or direction of the Board within the powers and authority provided by the aforesaid Act, common law, and other relevant pieces of legislation. In line with the top-down approach, the Board of Directors will make certain broad ICT pronouncements or policy directives that should be established and implemented at an operational level. In other words, the Board of Directors will depart from the concept of the 'bigger picture', the comprehensive position, and most of the time it will serve as a point of departure where ICT policy initiatives are formulated and governed. In terms of the bottom-up approach, the Group ICT Steering Committee will, in line with the legislation and/or company policies, take certain matters to the Board of Directors for information or decision-making purposes. The composition of the Board of Directors' sub-committees will differ from one organisation to another. For the purpose of this study, it is suggested that the Aifheli Group's Board should have five sub-committees as follows: 1) audit; 2) nomination and compensation; 3) corporate governance; 4) investment; and 5) sustainable development.

The ***Audit Committee*** (see Tier in Figure 7.2, and block 5 & 8 in Figure 7.5), amongst others, is responsible for identifying and mitigating the risks and this should include ICT-related risks. The Audit Committee should approve information security policies and monitor compliance. This committee, should, on behalf of the Board of Directors, determine whether legal aspects have been integrated into information security policies. Historically, Audit Committees were also responsible for reviewing draft mid-year and annual financial statements, supervising the implementation of internal and external controls, and managing significant risks. Due to its enabling capabilities in business processes, the failure of ICT can pose huge reputational and financial risks to the organisation. Most divisions within the company will not function optimally in the absence of ICT services, and in the worst scenario, some of the divisions will not operate if the ICT infrastructure and systems fail. ICT also provides business intelligence to various people within an organisation. The Audit Committee should ensure that there are measures to determine data quality and integrity. The ICT services should always be available when users require access. The uptime of the network should always be reliable. A network that is constantly disrupted leads to poor user experience and negative financial implications in a profit-making organisation. The network should provide quality transmission to carry the traffic. If the transmission is poor, the service will be compromised and this may lead to negative customer experience. Insufficient transmission yields slower or degraded connections which can pose both reputational and financial risk to the company. It is not within the remit of the Audit Committee to become involved in the technical detail, but rather the committee should supervise the establishment and implementation of the information security-related policies.

The Nomination and Compensation Committee is responsible for advising the Board of Directors regarding people who can serve as either non-executive or executive directors. Due to the pervasiveness of the ICT role within the organisation and the lack of clarity regarding the boundaries between the typical 'business of Aifheli' and the 'business of ICT within Aifheli', it is advisable for the Nomination and Compensation Committee to ensure that, amongst the Non-Executive Directors, there is someone with a broad knowledge of ICT-related risks. This director does not have to possess technical skills, but should provide 'bigger picture' advice and supervision. The committee should also be involved in the appointment of the Group CIO. Traditionally, and in many organisations, the Group CIO reports to the Chief Financial Officer. This is problematic because the Group CIO will then not sit on the Group Executive Committee (Exco) and on the Board of Directors as one of the Executive Directors. Although the Chief Financial Officer will serve in the aforementioned organisational structures, he or she may not be well acquainted with ICT and this will inevitably disadvantage the Board, Exco and the ICT Department. Ultimately, the greatest disadvantage will be felt by the whole company. At the same time, the Group CIO should not just be technical; s/he should have a broad understanding of business imperatives. Figure 7.3 below reflects a typical skills set of the Group CIO.

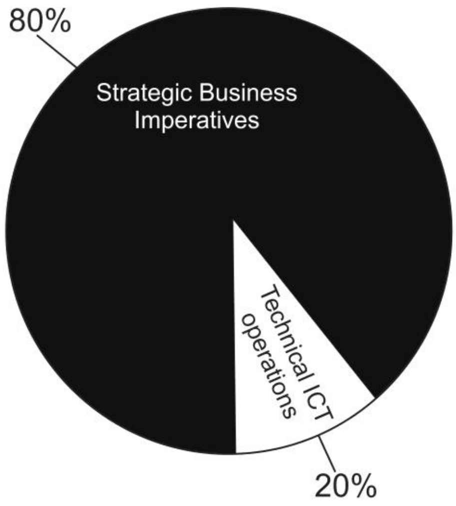


Figure 7.3: Diagrammatical Representation of the Group CIO disposition regarding Strategic Business and Technical Imperatives

The Nomination and Compensation Committee should appoint a Group CIO who will serve as a conduit between the business and ICT. At this level, the organisation needs a business leader rather than an ICT technical expert. The Group CIO should be more concerned with, firstly, how ICT strategy aligns with the overall organisational strategy; secondly, how ICT will add value to the competitiveness of the company; and thirdly, how ICT will contribute to the profitability and sustainability of the company. The Group CIO should be sensitive and conversant with the fact that ICT risks can damage the sustainability of the organisation. He/she should comprehend the significance of policies, procedures, and protocols in mitigating ICT risks. During the Board of Directors and Exco meetings he/she should be in a position to understand and articulate the ‘business language’. The Group CIO should also be able to translate ICT technical jargon into ‘business language’ and champion the role of ICT in the execution of the business strategy.

The Nomination and Compensation Committee should also appoint the Advisor to the Board and make recommendations for the succession of the Chairperson of the Board of Directors and some senior executives. This committee should also make recommendations regarding the compensation and benefits of the Board of Directors and senior executives, including, in relation to share options, stock subscription, and stock purchase mechanisms.

The ***Corporate Governance Committee*** should be responsible for the overall oversight of corporate governance by ensuring that the company’s operations are aligned to best corporate governance practice, overseeing the company's governance pronouncements, assessing the independence of the Non-Executive Directors, and establishing the ethical guidelines for directors and measures to deal with conflicts of interest. The Corporate Governance Committee may work in conjunction with the Audit Committee in determining ICT governance issues.

The ***Investment Committee*** should advise the company regarding its main strategic thrust. This committee will make recommendations on dealing with organic and/or acquisition growth, disposals, and strategic partnerships. In a situation where a majority shareholding is acquired, it will be essential for the Investment Committee to work with the Audit Committee in ensuring that ICT infrastructure and systems are connected to the newly acquired entity and that the legacy systems of the acquired entity do not pose information security threats to the Group.

The ***Sustainable Development Committee*** should ensure that the company approaches sustainability in an integrated manner by embedding economic, environmental and social aspects into the woven fabric of the Group. This committee should also ensure that its ICT operations do not contribute to environmental decay.

Almost all aspects of the ICT risk management responsibility have historically been placed under the ambit of the Audit Committee, although it is very clear that each of the Board of Directors' committees has either direct or indirect linkages with ICT risk management.

Tier 2: Group ICT Steering Committee

The Group ICT Steering Committee is illustrated as Tier 2 in Figure 7.2. This committee should be constituted by all the Executive Directors of the organisation. In the context of the Aifheli Group, members of the Group ICT Steering Committee will be the Group CEO, Chief Operations Officer, Chief Finance Officer, Chief Information Officer, HR (Human Resources) Executive, Legal Executive, Marketing Executive, Treasury Executive, Audit Executive, and the CEOs of the Group's four entities. (see Figure 7.1) The Group ICT Steering Committee should be chaired by the Group CEO and an independent advisor should be appointed to advise the committee.

The purpose of this committee is to:

- ensure that the ICT systems and infrastructure are in place to support the Board in the execution of its responsibilities with regard to good corporate governance, accountability, and business performance;
- ensure that the ICT strategy and all major ICT initiatives are aligned to the company’s business goals and success metrics;
- deal with ICT-related matters in accordance with the Board of Directors’ directives;
- identify ICT priorities in relation to the broad goals of the Group and with advice from CEOs of the four entities within Aifheli;
- pay attention to the ICT-related risks and governance issues;
- consider the reports from the Group CIO regarding the performance of the ICT function and budgets;
- determine the impact of ICT systems and infrastructure on business processes and performance;
- assume the highest level governance role over projects and consider reports of all projects and ICT initiatives in the Group;
- identify major strategic directions and matters with regard to the company’s needs in terms of ICT;
- determine, based on proposals presented by the Group CIO, the ICT policy framework and formulate and review the Group ICT programme in relation to all rolling capital projects underpinning the shared services and the core business of the company.
- The ICT Steering Committee should meet bi-monthly.

It is recommended that the Steering Committee should meet bi-monthly.

Tier 3: Group ICT Operations Committee (ICT OpsCom)

The ICT OpsCom appears as Tier 3 in Figure 7.2 and its members should be CEOs and two General Managers from each of the four entities of the Aifheli Group, the Group CIO, and the Group Chief Operations Officer. The ICT OpsCom should be chaired by the Group Chief Operations Officer and should meet monthly. The main purpose of the ICT OpsCom is to determine the ICT needs of the Group entities, identify gridlocks in business processes and ensure the effective co-ordination of the ICT rollout across the entire Group. The ICT OpsCom should also establish action plans to enhance the role of ICT in improving operations and to pay attention to ICT risks. Appropriate attention should be given to the deployment of ICT systems and infrastructure and the determination of proper controls to be maintained by each entity over the decentralised ICT systems. As part of exercising this responsibility, the ICT OpsCom should ensure that all the information security related issues are satisfactorily resolved. The ICT OpsCom should take into account and authorise various requests for minor changes to the ICT systems. It may consider some matters that have been forwarded to it by the Group ICT Steering Committee and ICT Entity Committees. On the other hand, it may also forward certain issues for consideration to the abovementioned governance structures. The ICT OpsCom should, where necessary, establish working groups and *ad hoc* sub-committees to deal with specific ICT operational matters. It should make recommendations to the Group ICT Steering Committee with regard to the ICT investments and operational matters with high impact in business performance.

Tier 4: ICT Entity Committees

Each of the four entities should have its own ICT committee chaired by the CEO. The Chairperson (entity CEO) should serve on the ICT OpsCom. Each ICT Entity Committee should be the main platform where the voices of users are heard regarding ICT issues within the entity. The ICT Entity Committee should submit ICT reports to the ICT OpsCom reflecting each entity's needs and concerns.

Other responsibilities of the ICT Entity Committees could be to:

- serve as a platform for the departments within the entity to share information about operational issues and how ICT can be an enabler;
- align the entity ICT activities to optimise ICT and determine the alignment with the Group Enterprise Architecture;
- assess the quality of ICT services on a quarterly basis and recommend service levels to the ICT OpsCom;
- provide input to the ICT OpsCom with regard to the crafting and implementation of the ICT plans and policies;
- monitor the ICT-related risks within the entity;
- serve as a safety vehicle to ensure there is a watch over ICT-related operations and that interventions can be made before crises arise; and

- co-ordinate the entity's activities regarding ICT and forward issues of interest and concern to the OpsCom.

The ICT Entity Committees will, where necessary, bring matters of concern and interest to the attention of the Group ICT Management Committee.

Tier 5: Group ICT Management Committee

The Group ICT Management Committee should be chaired by the Group CIO. Figure 7.4 below depicts a possible organisational structure of Aifheli's Group ICT Management.

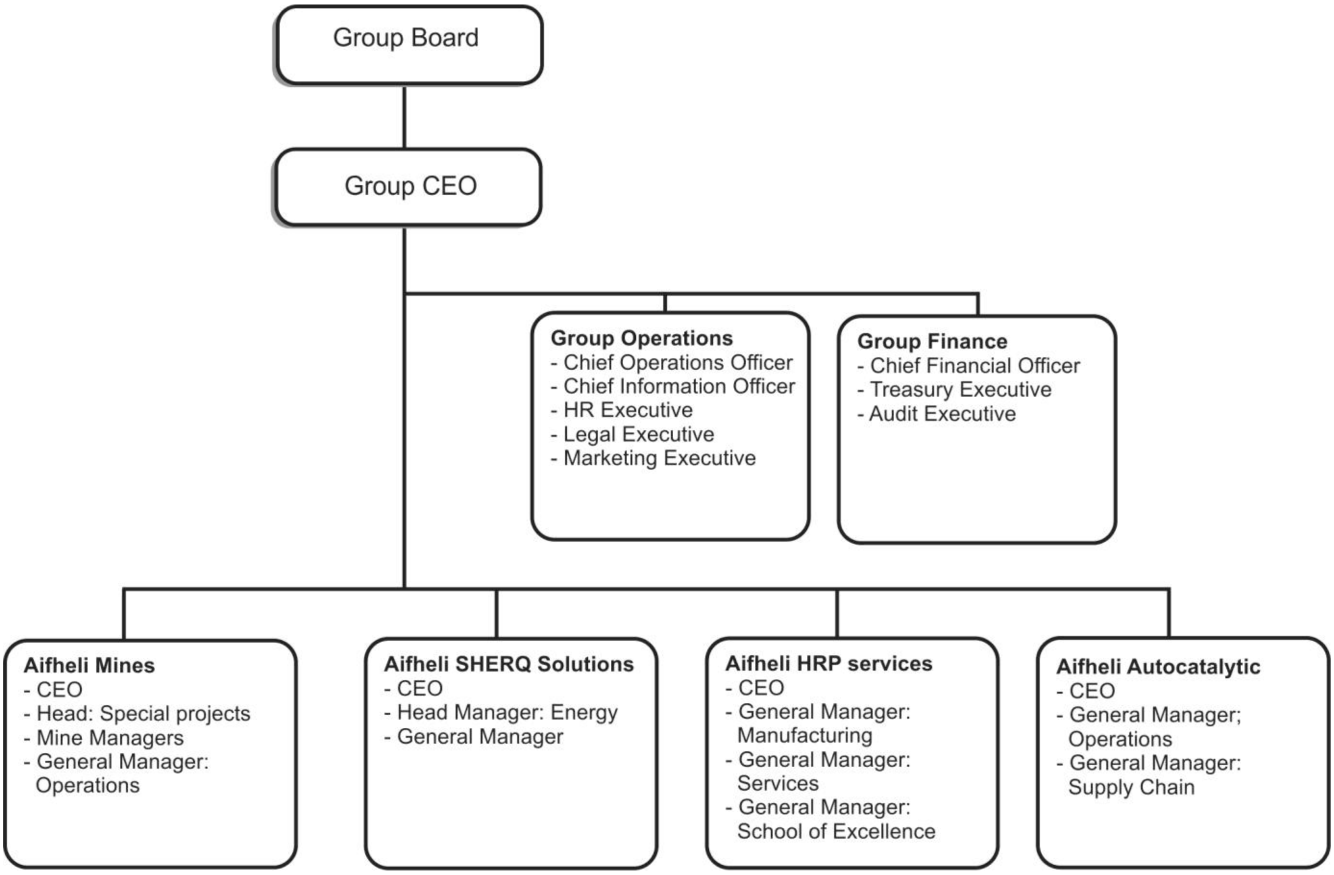


Figure 7.4: Diagrammatical representation of the Group ICT Management Structure (Source: Own)

As depicted in Figure 7.4 above, the Group ICT Management Committee should be constituted by the Group CIO and senior members of that office (Finance Manager, Programmes Manager, Project Manager, and an Independent Advisor), and Heads of Strategy and Governance, User Support, Infrastructure and Systems Solutions, and Enterprise Information Architecture. The remit of the Group ICT Management Committee is to:

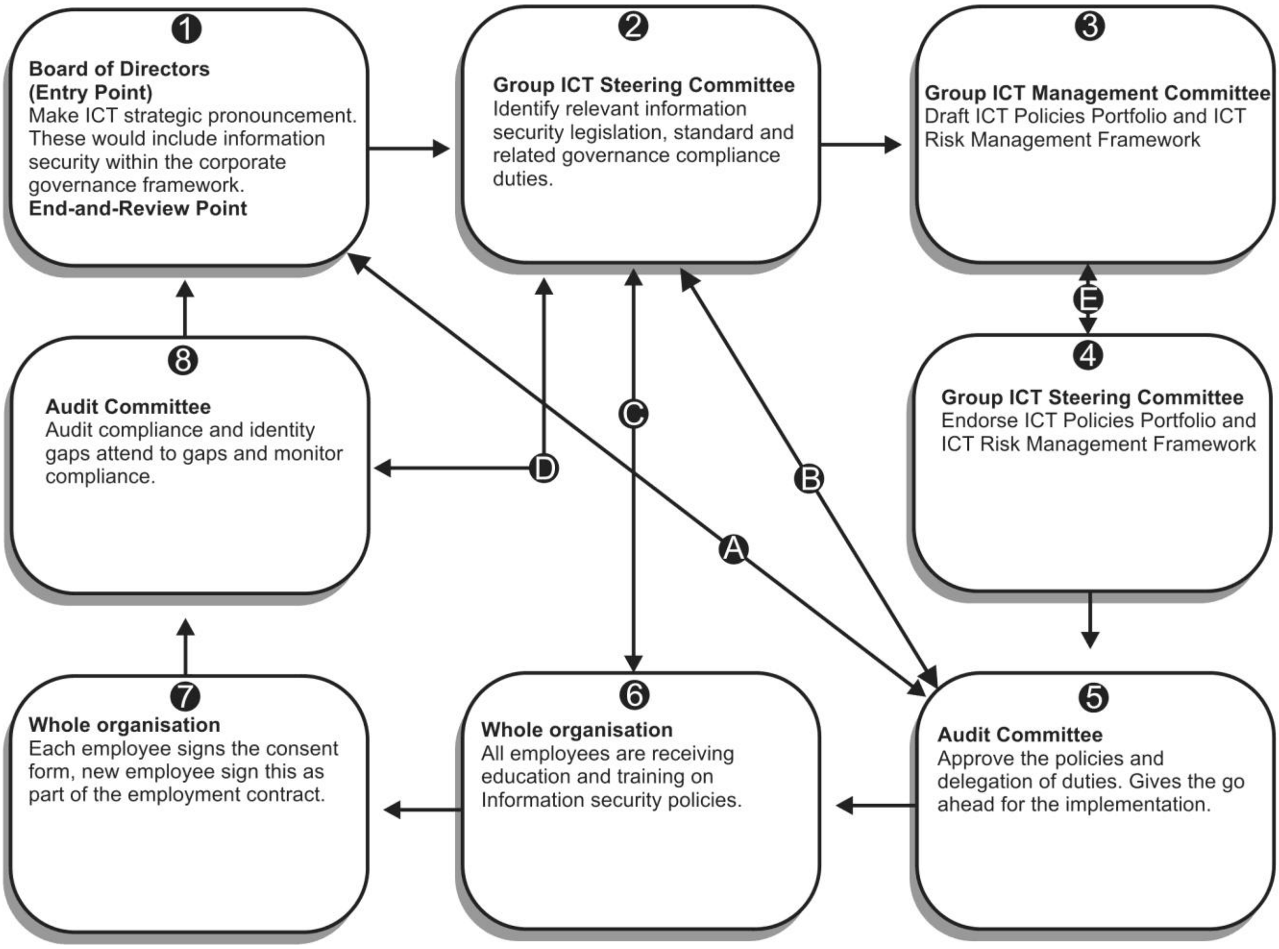
- align the ICT strategy with the overall Group strategy; implement enterprise-wide best practices and monitor trends globally, nationally, and within the Group;
- ensure that ICT initiatives are linked with business priorities; assume overall responsibility for the selection, procurement, deployment, support, and maintenance of infrastructure and systems;
- ensure that all ICT initiatives have clear business objectives and success metrics;
- conduct regular monitoring of the ICT skills of employees on behalf of the entities and the Group;
- make recommendations to the Group ICT Steering Committee regarding the alignment of ICT investments and strategic initiatives and operational needs of the entities and shared services;
- make recommendations to the Group ICT Steering Committee to approve the implementation of large-scale ICT programmes and projects;
- establish and deploy a consolidated ICT Service Delivery Model;
- establish and maintain an ICT Disaster Recovery and Business Continuation Plan and Procedure;
- establish and implement a draft ICT standards portfolio;
- establish and implement a draft ICT Risk Management Framework; and
- operationalise and implement decisions taken through approved recommendations and directives from other governance structures.

The next sub-section deals with the micro-organisational model implementation.

7.3.2 Micro-organisational model implementation

According to the King III Report (2009), enterprise strategic planning, risk management and information security are the primary responsibilities of the Board of Directors. It is not expected that the Board of Directors should be involved in a detailed process regarding the formulation of the information security policies, but they should make broader pronouncements within the business strategic direction and sustainability, corporate governance, standards, and legislation framework. Other role-players (components of the model) in the formulation, implementation, monitoring and evaluation are, Group ICT Steering Committee, Group ICT Management Committee, Board of Directors' Audit

Committee, and Whole Organisation. Figure 7.5 below illustrates the concept model regarding the placement of each governance structure in the process of integrating the legal aspects into information security policies and their implementation, and the interface between the governance structures.



1
Board of Directors
(Entry Point)
Make ICT strategic pronouncement. These would include information security within the corporate governance framework.
End-and-Review Point
2
Group ICT Steering Committee
Identify relevant information security legislation, standard and related governance compliance duties.
3
Group ICT Management Committee
Draft ICT Policies Portfolio and ICT Risk Management Framework
E
4
Group ICT Steering Committee
Endorse ICT Policies Portfolio and ICT Risk Management Framework
8
Audit Committee
Audit compliance and identity gaps attend to gaps and monitor compliance.
C
D
B
A
7
Whole organisation
Each employee signs the consent form, new employee sign this as part of the employment contract.
6
Whole organisation
All employees are receiving education and training on Information security policies.
5
Audit Committee
Approve the policies and delegation of duties. Gives the go ahead for the implementation.

Figure 7.5 Diagrammatical representation of Concept Model of Legal Compliance for Information Security at Corporate Environment (Source: Own)

The King III Report (2009) and the Companies Act No. 71 of 2008 require that a public company like the Aifheli Group should have a Board of Directors as the highest governance structure in the company (see block 1 in Figure 7.5). As discussed earlier, the Board of Directors may have committees that serve as working groups focusing on specific governance areas, such as the Group ICT Steering Committee (see block 2). Relevant information security and related compliance duties should be identified at this level. Once this has been done, the next governance structure is the Group ICT Management Committee (see block 3). The Group CIO, as the chairperson of this committee, should serve on both the Group ICT

Steering Committee and the Board of Directors as one of the Executive Directors. This would enable the Group CIO to take the identified information security legal provisions, requirements and related compliance duties and translate them into information security policies. The drafted information security policies will then be taken by the Group ICT Management Committee to the Group ICT Steering Committee for consideration and comment (see block 4). The Group ICT Steering Committee will allocate duties to the business units and/or individual positions. The policies will then be taken to the Board's Audit Committee (see block 5) for their approval. All employees will be trained regarding the information security policies (see block 6). They will also be asked to sign an Employee Acceptance Form, and the Employee Interception Consent (see block 7 and Paragraph VIII in this chapter). The Audit Committee will assess compliance and identify gaps (see block 8). Thus the overall intention of this model is the integration of legal aspects in the information security policies' formulation, implementation, monitoring, and evaluation, to elevate the benefits of business security, and ultimately address corporate security lapses.

Arrows named A, B, C, D and E in Figure 7.5 represent:

- When the Audit Committee (No. 5) approves policies and risk management framework, it should liaise with the Board of Directors (No. 1) for information purposes (see Paragraph VI). That is why there is an arrow named A connecting block number 5 and 1.
- The Audit Committe (No. 5) should also liase with the Group ICT Steering Committee (No. 2) to seek clarity and feedback and that is why these two blocks are connected by arrow named B) (See Paragraph VI).
- The Audit Committee (No. 8) audits the adherence to the security policies. The Audit Committee should work with the Group ICT Steering (No. 2) which is responsible for monitoring information information security compliance with the legal aspects (see Paragraph IX). The aforementioned blocks are linked by the arrow named D.
- If the Group ICT Steering Committee (No. 2) does not approve of policies portfolio and risk management framework, they should be taken back to the Group ICT Management Committee for improvement (No. 3) (see Paragraph VI). That is why there is an arrow (named E) connecting these two blocks.

Details of each component of the model

In this section, each component of the legal compliance model model is fully described. It has already been indicated in a previous section that these components are the Board of Directors, the Group ICT Steering Committee, the Group ICT Management Committee, the Board of Directors' Audit Committee, and the whole organisation.

a) Board of Directors (No. 1 in Figure 7.5) gives directives regarding ICT policies

It has already been mentioned that, as part of performing its duties, the Board of Directors should give directives for the establishment of organisational policies, including information security related policies, in line with the Group strategic direction. ICT plays an important role in the functioning of a company; its failure can threaten the sustainability of the organisation and therefore the Board of Directors should articulate broad ICT policy directives. The Board of Directors does not have to become involved in the technical details of such pronouncements.

In its endeavours to conform with legislation, the Board of Directors should be familiar with ICT risks as outlined in the literature, King III Report (2009) and Buys attorneys (2006): liability, risk or harm resulting from employees' abuse of electronic communication; risk resulting from a website and/or e-commerce; risk resulting from theft of ICT equipment; risk resulting from software; and risk presented by the failure of the Board of Directors and/or company executives to deal with information security breaches. The King III Report (2009) and the Companies Act No. 71 of 2008 explicitly identify risk management as part of the Board of Directors' responsibilities. Company management is accountable to the Board of Directors for crafting, implementing and monitoring ICT policies in general and specifically information security policies. Due to the pervasiveness and the critical role of ICT in the running of the company, one of the responsibilities of the Board of Directors is to educate and acquaint themselves with the ICT risks and how they can be mitigated through the integration of legal aspects in information security policies. Should the Board of Directors fail to educate themselves and the company consequently experiences major ICT breaches, the directors could, in their individual capacities, be held liable and the governance-related provisions of the Companies Act No. 71 of 2008 will become applicable. Some of the provisions in the aforesaid Act require a high level of compliance and personal responsibility on the part of a prospective non-conformance non-executive or executive director. There are many provisions in the Act detailing directors' liabilities. Prevailing concerns are exacerbated by the fact that directors can face litigation in their own personal capacity for almost any information security breach resulting from the negligence to educate themselves and ensure that the company is complying with the law. Given the liabilities placed on directors, any Board of Directors would be negligent in omitting to acquaint themselves with the requirements of the law regarding information security. The Board of Directors should conduct workshop(s) dealing with ICT-related risks and policies.

It is also the responsibility of the Board of Directors and its various committees to ensure that the Group complies with the legislation of the Republic. As discussed in previous chapters, there are several pieces of legislation that have a direct impact on the manner in which information security policies should be crafted and implemented (see Table 7.1). The Board of Directors should not necessarily mention each policy and the legislation aspects that should be integrated into it, but rather the Board of Directors may require the Group CEO to ensure that the following areas of information security are addressed in terms of policy implementation: hacking, intellectual property, copyright, protection of trademarks, privacy, and patents protection. The reason for the Board of Directors to delegate this responsibility to the Group CEO is because, in essence, the Board has only one employee – the Group CEO. That is why, if a significant information security incident occurs, the Board of Directors will require the Group CEO to account rather than the Group CIO. At the same time the Group CEO depends on other executives to carry out his/her responsibilities and thus there is a Group ICT Steering Committee.

b) Group ICT Steering Committee (No. 2 and 4 in Figure 7.5) identifies security areas and instructs the ICT Management Committee to establish an ICT Governance Portfolio

Almost all members of the Group ICT Steering Committee serve on the Board of Directors as executive directors and thus the provisions of the Companies Act No. 71 of 2008 and the King III Report (2009) related to directors' responsibilities and liabilities are applicable to them. The new responsibilities and liabilities placed on directors by the Companies Act have rendered the responsibilities of South Africa's executives similar to those of their counterparts in the United States, where they have been subject to the governance and reporting responsibilities contained in the Sarbanes-Oxley Act of 2002.

As discussed in a previous section, this committee, in essence, is actually the Group Executive; it is merely that, in this instance, the agenda of the meetings only focuses on ICT-related matters. Once the Board of Directors pronounces certain policy directives, it is the responsibility of the Group ICT Steering Committee to delegate the actualisation of these directives to individuals and/or structures. In this case, the Group ICT Steering Committee will delegate the responsibility of crafting information security policies to the Group CIO and the Group ICT Management Committee.

The Group ICT Steering Committee should require the Group ICT Management Committee to address information security areas (hacking, intellectual property, copyright, protection of trademarks, privacy, and patents protection) by establishing the ICT Governance Portfolio which is in line with the legislation of the Republic of South Africa and the best-of-breed national and international standards.

c) Group ICT Management Committee establishes an ICT Governance Portfolio (No. 3 in Figure 7.5)

The composition of this committee was outlined in Section 7.3.1. This committee has to put details regarding the mandate from the Group ICT Steering Committee in place by establishing the ICT Governance Portfolio. The committee should be sensitive to the fact that ICT Governance is a critical component for an effective ICT strategy and function. It is on this basis that ICT Governance should be documented and communicated to the Group to enable full implementation and compliance. A critical element of ICT Governance is the accountability in terms of information security. On the other hand, the Group ICT Management Committee should ensure that ICT functions are within a framework of policies and legal aspects. The lack of policies which integrate legal aspects disadvantages a structured growth of the ICT function within a Group and threatens its sustainability. This should be attributed to the fact that the organisation would not be operating in a normalised operating environment. With the exception of policies which integrate policy aspects, ICT Governance should be constituted by the establishment of operating standards, identifying the operational risks, and comprehending the whole notion of quality management and alignment with the critical success factors for ICT initiatives (vision, people, process, and technology). However, for the purposes of this study, the focus will be on the establishment and implementation of the ICT Governance Portfolio (Information Security Policies Portfolio and the Risk Management Framework).

d) Establishment of an ICT Policies Portfolio (No. 3 in Figure 7.5)

As illustrated in chapters 5, 6 and 7 of this thesis, the Group ICT Management Committee should acknowledge that there is a range of legislation in place that compels all organisations in South Africa, regardless of the method and form of their incorporation or founding, to comply with the provisions of the legislation in the implementation of information security. This requirement is applicable to all companies as defined by the Companies Act No. 71 of 2008, whether for profit companies (state-owned company, a private company, a personal liability company, or a public company) as well as not-for-profit companies.

The King III Report (2009) furthermore argues that information security is a critical component of the overall business and sustainability and thus companies should address information security by addressing confidentiality, integrity and availability. The Managing Director (Legal Firm 3) emphatically stated that the lack of awareness of the law cannot be used as a justification for corporate inefficiency pertaining to ICT risk and non-compliance with legislation.

The Group ICT Management Committee should take cognisance of the fact that, comprising a predominant part of corporate ICT governance, ICT policies which integrate legal aspects in terms of information security will guide the Group position on matters pertaining to ICT operations and others. This is because ICT permeates the company at all levels and enables the flow of the business processes. Due to ICT's pervasive nature, employees' work tends to revolve around ICT and in most instances information security and its relevant pieces of legislation are neglected and this leads to corporate non-compliance. To avoid this, the Group ICT Management Committee must establish an ICT Policies Portfolio by aligning information aspects with the relevant policies and legislation. Table 7.1 below illustrates this recommendation.

Table 7.1: Synopsis of ICT Policies Portfolio

AREA OF INFORMATION SECURITY	RELEVANT POLICY	RELEVANT LEGISLATION
1) Hacking	• Information security Policy • Data Privacy Policy • Access to Information Policy • Interception and Surveillance Policy • Records Management Policy • E-Commerce Policy	• Promotion of Access to Information Act No. 2 of 2000 • Electronic Communications and Transactions Act No. 25 of 2005 • Regulation of Interception of Communications and Provision of Communication related Act No. 70 2002 • Common law
2) Intellectual Property and Copyright	• Intellectual Property Policy • Information Security Policy • Data Privacy Policy • Plagiarism Policy • Records Management Policy	• Intellectual Property Law Amendment Act No. 38 of 1997 • Copyright Act No. 98 of 1978 • Merchandise Act No. 17 of 1941 • Films and Publications Act No. 65 of 1996 • National Archives and Records Service of South Africa Act No. 43 of 1996 • Promotion of Access to Information Act No. 2 of 2000 • Electronic Communications and Transactions Act No. 25 of 2002
3) Protection of trademarks	• Intellectual Property Policy • E-Commerce Policy	• Intellectual Property Law Amendment Act No. 38 of 1997 • Copyright Act of 1978 • Merchandise Act No. 17 of 1941
4) Privacy	• Data Privacy Policy • ICT Acceptable Use Policy • Electronic Communications Policy • Interception and Surveillance Policy	• Constitution of the Republic of South Africa Act No. 108 of 1996 • Protection of Personal Information Bill No. 9 of 2009
5) Patents protection	• No company had a distinguished policy on patents rights	• Patents Act No. 57 of 1978 • Note: Only three organisations addressed patents protection as part of their Intellectual Property Policy • Common law • Intellectual Property Rights from Publicly Financed Research and Development Act No. 52 of 2008.

The proposed ICT Policies Portfolio in Table 7.1 above adequately addresses the findings of this study as presented in Chapter 5 and 6. It also addresses ICT risks as described by Buys Attorneys (2006) as follows: liability, risk or harm resulting from employees' abuse of electronic communication; risk resulting from a website and/or e-commerce; risk resulting from theft of the ICT equipment; risk resulting from software; and risk presented by the failure of the Board of Directors and/or company executives to deal with information security breaches. Table 7.2 below demonstrates how risks identified by Buys Attorneys (2006) are addressed in the ICT Policies Portfolio.

Buys Attorneys (2006) also mentioned the risk associated with the failure of the Board of Directors and/or the company's management; this has not strictly been addressed in Tables 7.1 and 7.2. However, measures to deal with the negligence of both non-executive and executive directors are adequately provided for in the Companies Act No. 71 of 2008 and the provisions of this Act should not necessarily form part of any information security policies. Other than integrating legal aspects into the information security policies, ICT standards should also be integrated into some policies.

Table 7.2: Accommodation of ICT risks in the ICT Policies Portfolio

ICT RISKS	RELEVANT POLICY	RELEVANT LEGISLATION
1) Hacking (Buys Attorneys: employees risk, e-commerce risk, risk, & theft)	• Information security Policy • Data Privacy Policy • Access to Information Policy • Interception and Surveillance Policy • Records Management Policy • E-Commerce Policy • Information Security Standards Management Policy • Procedures Development and Management Policy • Quality Management Policy	• Promotion of Access to Information Act No. 2 of 2000 • Electronic Communications and Transactions Act No. 25 of 2005 • Regulation of Interception of Communications and Provision of Communication related Act No. 70 2002 • Common law
2) Intellectual Property and Copyright (Buys Attorneys: employees risk, E-Commerce risk, risk & theft)	• Intellectual Property Policy • Information Security Policy • Data Privacy Policy • Plagiarism Policy • Records Management Policy	• Intellectual Property Law Amendment Act No. 38 of 1997 • Copyright Act No. 98 of 1978 • Merchandise Act No. 17 of 1941 • Films and Publications Act No. 65 of 1996 • National Archives and Records Service of South Africa Act No. 43 of 1996 • Promotion of Access to Information Act No. 2 of 2000 • Common law
3) Protection of trademarks (Buys Attorneys: employees risk, e-commerce risk, risk & theft)	• Intellectual Property Policy • E-Commerce Policy	• Intellectual Property Law Amendment Act No. 38 of 19997 • Copyright Act of 1978 • Merchandise Act No. 17 of 1941 • Common law
4) Privacy ((Buys Attorneys: employees risk, E-Commerce risk, risk & theft)	• Data Privacy Policy • ICT Acceptable Use Policy • Electronic Communications Policy • Interception and Surveillance Policy • E-Commerce Policy • Information Security Standards Management Policy • Procedure Development and Management Policy • Quality Management Policy	• Constitution of the Republic of South Africa Act No. 108 of 1996 • Protection of Personal Information Bill No. 9 of 2009 • Common law
5) Patents protection (Buys Attorneys: employees risk, E-Commerce risk, risk & theft)	• No company had a distinguished policy on patents rights	• Patents Act No. 57 of 1978 • Notes: Only three organisations addressed the patents protection as part of the Intellectual Property Policy • Common law • Intellectual Property Rights from Publicly Financed Research and Development Act No. 52 of 2008.

e) Establishment of an ICT Risk Management Framework (No. 3 in Figure 7.5)

Since ICT is pervasive throughout Group entities and is an enabler to the business processes and connected to suppliers and customers, the Group ICT Management Committee should establish measures to mitigate information security threats. These measures should be implemented in line with the established ICT Portfolio. In essence, the best mechanism to counteract ICT threats is to actually implement the approved policies. At face value, the point being made sounds obvious, but practically it is not so apparent. During the fieldwork of this study, it was found some companies that had well-crafted policies, but which were never implemented, and these companies experienced a serious disjuncture between the policy and the actual implementation of information security. The proposed ICT Risk Management Framework should comprise the standards, procedures and quality management.

Standards can bring stability in the ICT environment and give assurance to the company that their information security implementation has been implemented within the framework of best practice. Due to the fixed nature of the standards, it is advisable that they should be customised to the particular operational environment. However, customisation should not lead to a major departure from the core framework of the standard. Standards should form part of the ICT Risk Framework and consequently ICT Governance, and thus they should be managed centrally as a portfolio. Apart from integrating aspects of standards into various information security policies, the Group ICT Management Committee should develop an Information Security Standards Management Policy which should deal with the following aspects: information security areas to be standardised, typical deviation from standards, motivation and process for customisation, deployment of the standards portfolio, review of standards, Group ICT Management Committee remit and answerability, and non-acquiescence management. The following standards could form part of the ICT Risk Management Framework: ISO 9000/20000 (which relates to quality assurance in project implementation), ISO 38500 (which deals with the corporate governance of ICT), and ISO 27000 Family of standards (Information Security Management Standards).

Standard Operating Procedures should form part of the ICT Risk Management Framework. In the absence of operational procedures, it would become difficult to monitor information security performance and compliance with the relevant legislation aspects and standards. It is therefore proposed that a Procedures Development and Management Policy be established.

Over and above this, the Group ICT Management Committee should ensure that quality management is an integral part of information security implementation. The fact that information security deployment conforms to legislation, best-of-breed standards, procedures and quality management, gives certain assurances to the Group Executive and the Board of Directors. A Quality Management Policy should be established and become an integral part of the ICT Management Framework. Once the ICT Policies Portfolio and ICT Risk Management Framework have been established, the Group CIO should, on behalf of the Group ICT Management Committee, submit these to the Group ICT Steering Committee. It is advisable for the Group ICT Management Committee to seek the advice of the Group ICT Operations Committee and the ICT Entity Committee before they are passed to the Group ICT Steering Committee.

f) Group ICT Steering Committee endorsement of policies portfolio and risk management framework (No. 4 in Figure 7.5)

If the Group ICT Steering Committee, for whatever reason, does not endorse the Policies Portfolio and Risk Management Framework, they should be taken back to the Group ICT Management Committee (No. 3) for refinement (see arrow named E). However, once the ICT Policies Portfolio and ICT Risk Management Framework have been endorsed by the Group ICT Steering Committee, the Group CEO should, on behalf of the Group ICT Steering Committee, submit them to the Audit Committee for approval.

g) Board of Directors' Audit Committee (No. 5 in Figure 7.5) approves policies and risk management framework

The Audit Committee should ensure that the ICT Policies Portfolio and ICT Risk Management Framework that have been endorsed by the Group ICT Steering Committee did not leave loopholes that could compromise the performance and sustainability of the organisation. The Audit Committee should satisfy itself that measures to deal with ICT security risks are integrated into the overall company strategy and that various information security policies are aligned to this strategy. See arrow B Furthermore, information security policies should have integrated all relevant legislative provisions. The Audit Committee should also ensure that ICT-related risks and security threats are identified and mitigated. The Audit Committee should obtain the services and advice of an independent ICT Law Firm or auditing company in executing the assessment of information security policies.

The Audit Committee should check whether information security policies have been formulated to deal with risks and potential threats in a way that is commensurate with the organisation's vision, business priorities, and goals. In line with the recommendations of the King III Report (2009), the Audit Committee should also determine how information security policies address the following three areas: confidentiality (protecting sensitive information from unauthorised disclosure); integrity (safeguarding the accuracy of data, information and software); and availability (ensuring that information and vital services are available when needed). During this period of evaluating the policies, the Audit Committee should liaise with the overall Board of Directors for information purposes and the Group ICT Steering Committee to seek clarity and give feedback. That is why, in Figure 7.5, there is an arrow numbered A between the Audit Committee (block 5) and the Board of Directors (block 1), and another arrow numbered B between the Audit Committee (block 5)and Group ICT Steering Committee (block 2).

h) Group Human Resources (No. 6 in Figure 7.5) conducts employee training

If the Audit Committee is satisfied with the submitted policies, they will be approved, dated and signed by the board of directors, and the Group CEO will be informed and the policies will then be implemented in the whole organisation. The Group ICT Operations Committee and ICT Entity Committee should be involved when it comes to the technical aspects of the policies' implementation. The Group CEO will, on behalf of the Group Steering Committee, give a directive to Group Human Resources to conduct training with all staff members in all the Group entities.

When formulating a corporate Information Security Training Programme, Group Human Resources should take into consideration that ICT systems are dependent on employees. This is in line with Schneier's (2003) argument, in which he asserts that information security is more about people's behaviour than anything else. In other words, in a corporate environment, information security is about countering employees' intentional and unintentional actions and the harmful implications thereof. In spite of the propaganda from ICT suppliers about the necessity of information security technology, many essential information security actions cannot be automated and thus they rely on the correct usage by the employees. This means that companies are reliant on employees to attain a secure ICT environment. Due to the fact that humans are regarded by several authors (Stephanou, 2008;

van Niekerk & Von Solms, 2004; Stephanou & Dagada, 2009; Schneier, 2003) as the "weakest link" in the information security chain, there is an apparent need for Group Human Resources to make sure that staff members are properly trained regarding the correct implementation of, and compliance with, information security policies and IT systems. The objective should be for Group Human Resources to ensure that, firstly, employees are equipped with the necessary information security skills and knowledge, secondly, that they apply the skills and knowledge, and lastly, that they are not easily misled, and thereby conform to the information security policies.

As part of establishing or procuring a corporate Information Security Training Programme, Group Human Resources should take into account that a real threat in terms of ICT systems is that of insiders, employees and consultants. This is so because these people are permitted to have privileged access to the ICT systems, are familiar with internal processes of the Group, and possess some technical knowledge. Together, these factors present a considerable risk to the company. It is on this premise that information security awareness and training must be conducted to enable employees to understand the rationale of information security policies what they must do to adhere to them. This view is supported by Sood and Enbody (2013). Security awareness and information security policies compliance should be done on an ongoing basis, not just once off and for new employees

Group Human Resources should also ensure that the corporate Information Security Training Programme enables employees to understand that information security policies contain legal provisions and that violating them do not just mean violating the organisational rules, but may also constitute a crime since one would be disregarding legal provisions. In other words, over and above facing disciplinary action, the employee can be convicted of a crime in a court of law. The corporate Information Security Training Programme should include measures to assess the usefulness of the information security awareness and training efforts.

i) All employees accept security policies by signing Consent Forms (No. 6, 7 in Fig 7.5)

Once the awareness and training programmes have been implemented, each staff member should sign the Consent Form and Employee Interception Consent (see Appendix D) which will enforce employees' adherence to the principles of good corporate governance; conformance to safety and information security of the organisations' network; and ensure a secure and healthy working environment. The Consent Form will enable the company to monitor employees' activities related to the use of Group ICT systems when required. The company should take into consideration the fact that in South Africa, employees have the constitutional right to privacy and thus the Consent Form is a correct mechanism to balance information security objectives and also compliance with the Constitution of the Republic of South Africa No. 108 of 1996.

The Consent Form enables the employees to agree to the necessary undertakings. The Consent Forms should be signed by employees who are already within the organisation when information security policies are approved by the Board of Directors and also when they are amended. Provisions contained in the Consent Form should be part of the employment agreement for new employees. Group Human Resources, with the guidance of Group Legal Corporate Affairs, should determine steps to be taken when employees refuse to sign the Consent Forms. Such steps should be taken within the framework of acceptable human resources practices and the labour laws of the Republic of South Africa. Once employees have signed the Consent Forms and the policies have been implemented, the next step in the legal compliance chain will be the audit conducted by the Board of Directors' Audit Committee.

j) The Audit Committee audits adherence to the security policies (No. 8 in Figure 7.5)

Once policies have been implemented, the Group ICT Committee should constantly monitor information security legal compliance. However, the actual audit of compliance should be done by the Audit Committee on behalf of the Board of Directors because whilst monitoring is a management issue, auditing is a governance matter (see D in Figure 7.5). It is advisable for the Audit Committee to obtain external independent assistance when carrying out the audit. The audit should look at both the compliance by the employees, and the ICT infrastructure and systems.

It is a well-accepted corporate practice to measure policy compliance. Other than that, it is part of the Board of Directors' fiduciary duties to conduct various audits as part of governance responsibilities. Regarding human resources' compliance with the information security policies, it may be advisable to take guidance from Haar et al. (2014) who reasoned that employees' policies compliance can be determined by observing their behaviours and attitudes through conducting password cracking; doing interviews with employees at pause areas in order to obtain anecdotal evidence; tracking the number and nature of incidents reported before and after information security policies were implemented; conducting clean desk audits and distributing surveys or questionnaires in order to obtain input from employees. This may include following up to determine what employees remember and what worked.

ICT infrastructure and systems are devised as intrinsic units, but are actually prone to disappoint due to their digital nature, vulnerability to attacks, and their dependence on resources outside the ICT sphere of influence. It is on this premise that the Audit Committee should also audit the ICT infrastructure and systems to ascertain whether they satisfy the requirements of the information security policies and the established Risk Management Framework. As a starting point, the Audit Committee should assess to what extent the ICT security infrastructure is linked to the enterprise-wide risk management efforts, while simultaneously considering that ICT risks cannot always be defined based on the parameters articulated on a corporate level. Back-ups are very important in terms of mitigating ICT risks and information security threats and thus the audit team should test their performance and whether there is adequate off-site back-up and alignment with the business expectations for data recovery capabilities. As part of the audit, an assessment of the Information Technology General Controls (ITGCs) of the Group should be conducted.

There are several templates of the ITGCs on the Internet and in the literature (for example, the Institute of Internal Auditors, 2008); however the information presented in Table 7.3 (below) has been modified to suit the proposed Concept Model of Legal Compliance for Information Security in the Corporate Environment.

Table 7.3 Possible scope of the ITGCs (Information Technology General Controls) in the Management Framework

Objective		**Overview of procedures**
ITGCs Components: Those mechanisms that management has implemented, and uses, to manage the day-to-day activities of the ICT environment		
1.	Adequate policies & procedures exist for governing the day-to-day operations of the ICT domain.	Inspection of policies and understanding of procedures governing: • Information security administration; • incident monitoring; • change management; • backups; • batch/job processing; etc.
2.	A defined structure exists under which ICT operates.	• confirmation of organisational structure with a focus on understanding reporting structures, responsibilities and on ensuring key functions are segregated; • understanding and validation of key management meetings (including core audit) with a focus on understanding items discussed, and on the nature and format of documentation produced.
3.	An ICT strategy exists governing the short and long term goals, and the steps needed to achieve the goals.	Inspection of ICT strategy with a focus on understanding: • short term goals; • long term goals; • alignment with business; and • steps to be taken to achieve goals
Program Change Control: The process whereby changes are made to data, application functionality & reports		
4.	Only authorised individuals who have access to migrate changes into production, and these persons are segregated from those responsible for development activities.	• comparison of list of developers to those who are responsible for, and with access to, migrate changes into production; • validation of program listing to ensure all access is authorised, and that adequate segregation of duties exists between system developers and those responsible for migrating changes.
Access to Programs & Data: the process around ensuring application & data access is restricted to authorised individuals		
5.	User provisioning processes ensure that only authorised users have access to the applications and databases.	Validation of user provisioning processes with a focus on ensuring that: • all new users are approved; • accounts for terminated users are removed in a timely manner; • adequate segregation of duties exists between critical functions; and • regular reviews are performed on users with access to the shared applications and databases.

Objective		Overview of procedures
6.	Production servers are appropriately configured to reduce the risk of unauthorised access to the databases and shared applications.	Review of information security configuration for production servers. Review will be performed using proprietary scripts and will include the validation of high risk security configuration. This will include the review of: • audit logging configuration & associated monitoring procedures; • password parameters; • trusts & servers; and • accounts with administrative privileges.
7.	Administrative privileges are restricted to authorised personnel only and all activities performed with these accounts are authorised.	• Validation of persons with administrative access to application, and associated technical platforms; • Review of audit logging/monitoring procedures for users with administrative access.
Computer Operations: The process around ensuring adequate monitoring of the application environment is performed		
8.	Adequate procedures have been implemented to ensure adequate recovery in the event of the disaster.	• Review and validation of back-up schedule and associated monitoring; • Inspection of ICT environmental controls, with a focus on understanding mechanisms implementation to control the server environment; • Inspection of Disaster Recovery Plan (DRP), and review of procedures performed by management to ensure that DRP functions effectively.
9.	Production issues are monitored and resolved in a real time manner.	• Review and validation of job schedule and associated monitoring; • Validation of Help Desk monitoring/tracking procedures.

Adapted from Bytes Technology Group’s ITGCs Framework

The purpose of the ITGCs is to appraise key controls with the ICT general computerised control environment that supports reliable and continuous processing of computerised information systems, and secondly, to report to the Board of Directors the areas of perceived weakness or areas for improvement in procedure or control. The Board of Directors will delegate audited matters that need attention to the Group ICT Steering Committee for ratification and implementation.

7.4 SUMMARY

There is a general trend in organisations to place a low probability on ICT risks and data disaster occurrences. The reality is that ICT infrastructure is a high risk in itself, and thus a domino effect applies here, as the failure of infrastructure will, without doubt, also lead to the loss of data, information and business intelligence. Organisations should not perceive the establishment of information security policies, the ICT Risk Management Framework and the implementation thereof as a costly overhead which needs to be downgraded. This chapter recognises the critical significance of integrating legal aspects into information security policies and thus a Concept Model of Legal Compliance for Information Security in the Corporate Environment was presented in this chapter. It has been argued that the governance aspect of ICTs should be taken seriously by the Board of Directors and other governance structures and it should not be given a lower priority due to its technical nature. The alignment of the ICT strategy to the overall business strategy and the impact of ICT in the sustainability of the organisation should be interrogated.

Inasmuch as this chapter has been constructed around a hypothetical organisation in which the proposed Concept Model (of Legal Compliance for Information Security in the Corporate Environment) can be implemented, it is the researcher's view that this model can be implemented in actual companies, irrespective of their governance and management structures.

It was stated at the beginning of this chapter that the proposed Concept Model combined theory, the experience of the researcher as an academic and ICT Manager as well as cognitive perspectives gained over many years (see Section 7.1). It had also been indicated in Chapter 4 that this study was a product of the interplay between the philosophical outlook (researcher’s ontological position) and the empirical findings of the study (see Section 4.1). The researcher’s ontological perspective has influenced the research methodology used, and by implication, the findings of the study and the Concept Model.

The following chapter concludes the thesis, highlighting some limitations and giving possible recommendations.

CHAPTER EIGHT
OVERVIEW, CONCLUSION, LIMITATIONS AND RECOMMENDATIONS

8.1 OVERVIEW OF THE STUDY

This chapter contains the summary and conclusion of the research as well as further recommendations for practitioners and researchers.

This study has attained the objectives that were articulated in Chapter 1 as follows:

i. A literature review was undertaken to determine the nature of information security-related problems specifically pertaining to e-commmerce viz hacking, viruses, privacy, ethical issues and industrial espionage and the relevant South African laws pertaining to these mentioned information security issues (see Chapters 2 and 3).

ii. Fieldwork was conducted to determine firstly, the way in which South African companies are employing legislative imperatives in providing information security; secondly, the extent to which the South African legal framework impacts the formulation of information security policies at organisational level; thirdly, the extent to which South African companies are complying with the commercial websites' legal requirements, and lastly, to determine, by means of studying documents collected from the participating companies (policies, procedures and strategies) how they are incorporating legislation and policies into their information security measures (see Chapters 5, 6 and 7).

iii. A Concept Model of Legal Compliance for Information Security in the Corporate Environment was proposed in Chapter 7. This Concept Model embodies the contribution of the study (see Chapter 7).

As previously explained, many organisations and consumers are using the Internet for commercial purposes (e-commerce, financial transactions and the like). However, both the merchants and customers are vulnerable to information security risks. Through a brief literature review, the researcher argues that policy and legal aspects should be employed to enhance information security implementation in South Africa. The information security legal framework, specifically within the context of South Africa, was articulated.

The following statutory instruments were identified as dominant elements of the South African legal framework regarding e-commerce and information security in particular: the Constitution of the Republic of South Africa, No. 108 of 1996 (specifically the right to privacy); the Electronic Communications and Transactions Act, No. 25 of 2005 (which provides the framework behind electronic communications and also addresses cyber-crime - see Chapter 13, Sections 85-89); Promotion of Access to Information Act, No. 2 of 2000 (which deals with records management, disclosure, confidentiality and access); Regulation of Interception of Communications and Provision of Communication-related Act, No. 70 of 2002 (this Act prohibits the interception and monitoring of information without permission from a court of law); the Protection of Personal Information Bill, No. 9 of 2009 (which deals with the right to privacy); as well as the King Reports on Governance for South Africa (King II of 2002 and King III of 2009).

Based on the findings of this study, it was argued that most South African companies did not appear to be integrating legal and policy aspects as part of implementing information security, and this formed the basis of the research problem which required further investigation. The research question and two sub-questions emanated from the literature review and the research problem. The aim of the study was to assess how companies in South Africa were integrating legal and policy aspects when they deal with information security related issues. In order to achieve the aforementioned aim, the researcher undertook to embark on a literature review and field study. During the field study, data were collected and the data analyses thereafter were conducted within the parameters of qualitative research methodology.

The research question and its sub-questions have been answered in Chapter 5, 6 and 7. The findings of this study revealed that most companies in South Africa were not integrating legal aspects into the implementation of information security. It is on this basis that the researcher developed the proposed Concept Model of Legal Compliance for Information Security in the Corporate Environment. The Concept Model embodies the contribution of the study.

8.2. SUMMARY OF CONTRIBUTIONS

As a result of this study, theory has been generated in several ways. This is deemed essential for future work in the field of information security.

8.2.1 Theoretical contributions

Firstly, Chapters 2 and 3 have, by means of the literature study and legal framework, provided a typology for interlinking legislation requirements and policy formulation in the provision of information security in the South African context (see section 1.6). This typology can henceforth be used by Boards of Directors, ICT executives, information security practitioners, e-commerce participants, and policy formulators to enhance the provision of information security. A search of electronic databases and e-journal portals revealed no results pertaining to such a typology and thus one may claim that no such typology currently exists that has mapped, matched, and linked a specific information security problem with the applicable South African legislation, as in this study.

Secondly, the findings of this study, as contained in Chapter 5 and 6, extended information security theory in a number of ways which may lay a foundation regarding work being done towards the integration of legislation requirements and policies. The theory generated in these chapters revealed the importance of the following – the necessity of ensuring that the Board of Directors has the appropriate attitude towards information security-related governance; the role of policy formulators and government in providing a regulatory environment which enables companies to implement information security properly; the effects of regulatory compliance fatigue on users; and the importance of the applicable pieces of legislation in policy formulation and the implementation of information security.

Thirdly, the originality of the contribution of this study to the academic and industry knowledge base of information security benefited from additional contextualised corporate description that can augment the understanding of the complexities of employing legislation to enhance information security in the South African corporate environment.

8.2.2 Methodological contributions

This study has made a methodological contribution in the form of the Concept Model of Legal Compliance for Information Security in the Corporate Environment. Although the literature review and the findings of this study illustrated the operational and governance necessities for the integration of legal aspects into information security policy formulations, the abovementioned Concept Model did not exist prior to this research and thus it is a direct result of this study. The importance of the proposed Concept Model can be seen in its role of guiding South African organisations to implement information security within the broader framework of the applicable law.

The proposed Concept Model integrates legal requirements and information security operational needs into a single model. It was also demonstrated how the Concept Model can be operationalised by implementing it in a hypothetical organisation in South Africa. It is therefore the researcher's view that this model can be implemented in real organisations and thus it is transferrable. By crafting and demonstrating the implementation of this Concept Model which synthesises theory, the practical and philosophical outlook of the researcher gained over years of studying and practical experience, contributes to the information security methodological interventions. International organisations and foreign governments may find the proposed Concept Model useful. For example, multi-nationals can start with the South African laws and draw on the applicable laws of other countries where they operate.

This thesis has achieved something not previously undertaken by integrating two traditionally foreign concepts – information security and legislation requirements - into a single information systems methodological approach. This model was operationalised in Chapter 7. Before the two concepts were integrated in Chapter 7, the literature review and the findings chapters had presented detailed referencing to equip the reader with the theoretical and real-life grounding of legislation requirements pertaining to information security. The Concept Model thus embodies the main contribution of this study to information security knowledge.

8.2.3 Practical contribution to Boards of Directors in corporate South Africa

The study encourages corporate South Africa to take ICT governance and risk management seriously. It was found that the attitude of corporate South Africa towards the integration of relevant legislation into information security policies was generally negative (see Section 5.2.1). This thesis provided a literature review, empirical findings, and a Concept Model, all of which provide evidence and reasons as to why the Board of Directors should be involved in the formulation of ICT policies and execution oversight regarding the implementation thereof. This study makes it very clear that the involvement of the Board of Directors in this matter is not voluntary but rather compulsory since it is a legal and corporate governance requirement. Other than the Board of Directors, at an operational level, ICT governance cannot be relegated to an ICT manager or information security specialist, but should rather be dealt with at the level of the Group CEO, Group Executive Committee and the CIO. The ICT manager or information security specialist will handle the technical aspects of information security.

The integration of legal aspects into the formulation and implementation of information security is a relatively new concept in South Africa and this study found that organisations did not always know how to go about it; that is why a Concept Model has been proposed to serve as a reference point and guideline. As part of demonstrating how corporate South Africa can incorporate legal aspects into information security policies, this thesis dealt with the macro and micro facets of the organisational implementation of the Concept Model. At macro level, these would include the development and execution of the ICT Enterprise Architecture.

On the other hand, at micro level, this study illustrated aspects of the Concept Model and roles that should be played by the Board of Directors, Group ICT Steering Committee, Group ICT Management Committee, Board of Directors’ Audit Committee, and all employees in the establishment, implementation, monitoring and evaluation of information security policies.

Corporate South Africa will find it easy to implement or use the Concept Model as a reference point because it is generic in its disposition, product-independent and caters for both aspects of information security i.e. governance and operations. Depending on the nature of their information security legislation, this Concept Model can also be useful in other countries.

8.2.4 Practical contribution to executive management in corporate South Africa and worldwide

Through the findings contained in Chapter 5 and 6, this thesis reveals and advises executive management in companies to ensure that information systems users (employees, consultants and customers) are sufficiently aware and trained when it comes to implementing information security policies. In most companies that participated in this study, users had only an elementary knowledge of information security policies. The executive management team should be seen to take information security policies seriously so that all the other employees and users emulate them. On the other hand, the awareness programmes should not be done superficially merely to satisfy the audit requirements. The executive management should assist the Board of Directors by implementing and monitoring compliance with information security policies on a day-to-day basis.

8.2.5 Practical contribution to policy formulators

South Africa is a constitutional state and thus the Constitution of the Republic is the supreme law of the country. All laws in South Africa should derive from this legal construct and be aligned with the constitutional framework. In South Africa, there are three major organs of state – Executive, Parliament and Judiciary. The Executive (Cabinet) is responsible for articulating policies, co-ordinating them into laws and overseeing implementation thereof once the legislature has approved them. Other than approving the Executive's policies, Parliament (legislature) also represents the public, approves laws, and monitors the work of the Executive. The judiciary's authority is predetermined in the Constitution of the Republic of South Africa. The role of the judiciary is to exercise judicial authority over the Republic. Based on the aforementioned background, 'policy formulators' in this study refers specifically to both the government and parliament. Through the findings of this study, policy formulators were advised:

- To ensure that legal provisions to fight cyber-crime are not redundant. These include provisions contained in Chapter 8 of the Electronic Communications and Transactions Act, No. 25 of 2002. These provisions deal with unauthorised access to, interception of or interference with data and thus they are supposed to be tackled by the cyber inspectors.

At the time of writing this document, the appointment of the cyber cops has not yet been implemented and this study urges policy formulators to effect the appointments.

- To implement the establishment of the cryptography service providers in line with Chapter 10 of the Electronic Communications and Transactions Act, No. 25 of 2002.
- To implement the provisions of the Intellectual Property Law Amendment Act, No. 38 of 1997 by arresting people responsible for extensive music and video pirating.
- To speed up the implementation of the Protection of Personal Information Bill, No. 9 of 2009.
- To amend the Patents Act, No. 57 of 1978. This Act was passed many years ago before the Internet was used for commercial purposes and thus there is a need to update the law through amendment. This Act states that software patents cannot be patented in South Africa. It is on this premise that policy formulators are urged to amend this position because it has led to the unintended consequence of discouraging ICT multinationals from directly investing in South Africa because they fear their patents will not be protected. However, before the Patents Act, No. 57 of 1978 is amended, government should ensure that the law is enforced. So far this Act has been ineffectual because, although it stipulates that computer programmes cannot be patented, companies and individuals have been registering software-related patents with CIPRO, now CIPC (the Companies and Intellectual Property Commission).

8.3 IDEAS AND IMPLICATIONS FOR FUTURE RESEARCH

Several ideas emerged for future studies. Firstly, future research can build and extend on the findings of this study using objective measures to gauge the effectiveness of information security policies. Further research could also investigate additional or alternate contextual factors and could employ a longitudinal approach to examine the integration of legal aspects into information security policies. Information security governance and the implementation of the Concept Model that has been suggested in this study require a reasonable time period to implement and consequently to test the application of the model; for that reason longitudinal case studies may prove to be effective. Further longitudinal studies may provide important insights into the effectiveness of statutory instruments that predominantly regulate the South African legal framework regarding e-commerce and information security, and in particular the Constitution of the Republic of South Africa, No. 108 of 1996 (specifically the right to privacy); Electronic Communications and Transactions Act, No. 25 of 2005 (which provides the framework behind electronic communications and also addresses cyber-crime – chapter 13, sections 85-89); Promotion of Access to Information Act, No. 2 of 2000 (which deals with records management, disclosure, confidentiality and access); the Regulation of Interception of Communications and Provision of Communication-related Act, No. 70 2002 (which prohibits interception and monitoring without judicial permission); the Protection of Personal Information Bill, No. 9 of 2009 (which deals with the right to privacy); and the King Reports on Governance for South Africa (King II and III).

Secondly, certain laws which have an impact on information security policies were not yet passed when this study was finalised or were only passed just before this study was concluded. Therefore further research should examine their impact on the implementation of information security. These include the Companies Act, No. 71 of 2008 (which only became effective on 1 May 2011) and the Protection of Personal Information Bill, No. 9 of 2009, which was signed into law (PoPI Act No. 4 of 2013) on 27 November 2013.

Thirdly, further research could also focus on the role that the National Consumer Commission (NCC) plays regarding consumers' infringements in respect of complaints that emanate from the merchants' failures to integrate legal aspects into their information security implementation. The NCC was established in terms of section 85 of the Consumer Protection Act, No. 68 of 2008 as an organ of the state, but carries out its mandate outside of the public service. It is the researcher's view that there will be cases against companies for infringements that violate the act as follows: failure by the merchant to provide a fair, accessible and sustainable marketplace, and unfair online marketing and business practices.

Fourthly, further research should investigate the impact of legal aspects and information security policies in promoting responsible consumer behaviour. Lastly, future research should focus on the potential obstacles (such as the cost, or the politics) of implementing the proposed concept model in the corporate environment (see Paragraph 8.4).

8.4 LIMITATIONS OF THE STUDY

Firstly, it was difficult to conduct a study within the parameters of the information systems terrain without encroaching into the legal field. It was not the intention of this study to interpret the law, but rather to investigate the integration of legal aspects into information security policies. The researcher has, however, at the beginning of this thesis stated the IANAL principle of, “I am not a lawyer”, emphasising that this research is not a legal study but rather an information systems study. In some instances, it became very difficult to undertake the aforesaid investigation without providing some legal context and appearing to be interpreting the law, especially in Chapter 3. The danger of this action is that the possibility of interpreting the law incorrectly is very high because the author is not a lawyer. This study was scrutinised by lawyers but despite this, the responsibility to ensure the validity of the study remains with the researcher, and where a certain clause of the law could have been misinterpreted, this remains the responsibility of the researcher.

Secondly, it was difficult to conduct focus group interviews as part of qualitative data collection methods in this study. During the proposal stage of this study it was envisaged that at least six focus interviews would be conducted. However, it was not possible to have groups of 12 information security practitioners in the same room at the same time. Attempts to piggy-back on conferences and seminars did not yield any fruitful results because organisers could not accommodate requests due to various reasons.

Thirdly, to a certain extent, the depth of the study would have been enhanced with more than one interviewee from each organisation. It was, however, difficult to obtain permission from the organisations. Moreover, the researcher would have been overwhelmed by the requirements in both time and cost of conducting more than one hundred interviews.

Lastly, although this study proposed a concept model which will address the legal requirements of organisations in the corporate environment with respect to information security, how this would be implemented in the corporate environment does not include potential obstacles, for example cost, politics, or similar. It would, however, not have been possible to do this without the concept model actually being implemented and thus one of the recommendations for future research addresses this aspect (see § 8.3).

8.5 CONCLUSION OF THE STUDY

The findings of this study indicate that most organisations in South Africa are not integrating legal aspects into information security policies. Such integration of legal aspects into information security policies is an important element regarding the adherence to the law and to tightening information security in the corporate environment. One of the most important outcomes of this study is the proposed Concept Model of Legal Compliance in the Corporate Environment. This Concept Model embodies the contribution of this study and demonstrates how legal requirements are incorporated into information security endeavours. The fact that the proposed Concept Model is technology-independent and that it can be implemented in a real corporate environment, irrespective of the organisation's governance and management structure, holds great promise for the future of information security both in South Africa and abroad. Furthermore, this thesis has generated a typology for incorporating legislation related to the provision of information security which can be used by any academic or practitioner who intends to implement information security measures in line with the provisions of the South African law. If this study proves that legal aspects are significant in the provision of information security, practitioners can to some extent construe that the integration of legislation into information security policies can be done in other South African organisations that did not participate in this study. In reality, however, there is still much research work to be done in this area.

In concluding this study, the author is, like Coetzee (1999), humbled by the consciousness that what has been achieved in this small project is but a very small drop in the ocean of scholarship and that the following applies:

The learning journey:

Although finalising the study, the learning journey has only just commenced. Appreciating the enormity of what has been proposed in this thesis enforces the belief that much must still be written, much requires further study and that the final word will lie in the collaborative effort of scholars. During the production of the thesis, ideas and processes were subjected to peer review and discussions to establish credibility in the study. This was achieved by publishing the following papers:

- Dagada, R., Eloff, M.M. & Venter, L.M. 2009. *Too many laws but very little progress! Is South African highly acclaimed information security legislation redundant?* ISSA 2009 Conference. University of Johannesburg, 6 to 8 July 2009.
- Dagada, R. & Eloff, M.M. (2013). Integration of policy aspects into information security issues in South African organisations. *African Journal of Business Management*, 7(31), 3069-3077.

In 2009, the researcher presented a paper entitled "*Legal and policy aspects to consider when providing information security in the corporate environment*", at the School of Computing 2009 Post-Graduate Symposium, held at the University of South Africa, 14 September 2009. This paper was rated as the best doctoral study presentation.

Ideas, the seeds of innovation:

Thoughts and ideas expressed in this thesis will make a difference if shared, tested, refined, implemented and reviewed. Within the boundaries of this academic contribution lie many seeds, which over time can be taken up by others so as to ensure that they materialise into more than just a Concept Model. It is the view of the researcher that this study will contribute to an increased understanding on the part of scholars and practitioners, with the possibilities of expanding on the study topic.

Conceptualisation, the basis for realisation:

Reality is today, concepts are the future. Influencing the future will be impacted by current knowledge; the extent to which dreams and ideas are integrated into future realities will determine the extent to which people are able to survive as knowledge workers.

--o0o--

REFERENCES

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Infromation Technology,* 33(3), 236-247.

Abdullah, N., Xu, Y., & Geva, S. (2013). Integrating collaborative filtering and matching-based search for product recommendations. *Journal of Theoretical and Applied Electronic Commerce Research, 8(2), 34-48.*

Adrian, A. (2013). Could a small town in Romania bring Australia to its cyber-knees? Not if they accede to the EU convention on cybercrime. *Journal of International Commercial Law & Technology,* 18(3), 328-338.

Agwu, E. (2013). Cyber criminals on the Internet super highways: a technical investigation on different shades and colours within the Nigerian cyber space. *International and Colours within the Nigerian Cyberspace,* 3(2), 56-74.

Alazab, M. & Venkatraman, S. (2013). Detecting malicious behaviour using supervised learning algorithms of the function calls. *International Journal of Electronic Security and Digital Forensics,* 5(2), 90-109.

Aleshnikov, S. & Demin, S. (2013). Problems of information security of the firm and a way of their decision. *Vestnik IKBFU,* 10(2), 147-154.

Alvesson, M. and Skoldberg, K. (2000). *Reflexive methodology: new vistas for qualitative research*. London: Sage.

Andoh-Baidoo, F.K., Osei-Bryson, K.M. & Amoako-Gyampah, K. (2012). Effects of firm and IT characteristics on the value of e-commerce initiatives: an inductive theoretical framework. *Information Systems Frontiers,* 14(2), 237-259.

Ardito, L. & Procacciant, G. (2013). Smart grid technologies in Europe: an overview. *Energies,* 6(1), 251-281.

Assaf, K. (2012). Magical thinking in trademark law. *Law & Social Inquiry,* 37(3), 595-626.

Bagby, J.W. (2003). *E-commerce law: issues for business.* Ohio: Thomson.

Bakker, B. (2007). *Software patents: IP or not IP*. Brainstorm. Sandton: ITWeb.

Bedard, D. (2014). Three ways to enchant your customers with ecommerce. *Journal of Multidisciplinary Research, 4(2),* 17-29.

Behr, L. (2013). Trademarks for the cure: why nonprofits need their own set of trademark rules. *Boston College Law Review,* 54(1), 243-274.

Bellovin, S.M. (2013). Military cybersomethings. *IEEE security and privacy,* 11(3), 88-99.

Berman, P.J. Reister, A.G. & Kregel, S. (2003). E-commerce patents. In: Plotkin, M.E., Wells, B. & Wimmer, K. (eds.) (2003). *E-commerce Law & Business* (Volume 1). New York: Aspen Publishers, 6.1-6.136.

Bertens, L.C.M., Broekhuizen, B.D.L. & Naaktgeboren, C.A. (2013). Use of expert panels to define the reference standard in diagnostic research: a systematic review of published methods and reporting. *PLoS Medicine,* 10(10), 1-17.

Berti, J. & Rogers, M. (2004). Social engineering: the forgotten risk. In: Tipton, H.F. & Krause, M. (eds.) (2004). *Information Security Management Handbook*. London: Auerbach Publications, 147-154.

Bin-Baba, M.S., Tamjid, H. & Gholipour, R. (2013). Information security – professional perceptions of knowledge-sharing intention under self-efficacy, trust, reciprocity, and shared language. *Computers & Education*, (68), 223-232.

Borgmann, A. (2013). So who am I really? Personal identity in the age of the Internet. *Al & Society,* 28(1), 15-20.

Bowers, B., Cohen, L.W. & Elliot, A.E. (2013). Creating and supporting a mixed methods health services research team. *Health Services Research*, 48(6), 2157-2180.

Brenner, J.F. (2013). The growing threat of cyber attacks on industrial control systems. *Bulletin of the Atomic Scientist*, 69(5), 15-20.

Burda, D. & Teuteberg, F. (2013). Sustaining accessibility of information through digital preservation: a literature review. *Journal of Information Science, 39(4), 442-458*.

Buys Attorneys. (2006). *ICT risk checklist with legal, IT and corporate governance solutions* (Second Edition). Cape Town: Buys Inc. Attorneys.

Buys, R. (2004). *South African website compliance survey results nothing to be proud of.* Buys Inc. Attorneys/Legalsentry.

Buys, R. (2005). *Biggest hack attack in South African history*. Buys Inc. Attorneys/Legalsentry.

Calafiore, G.C., Dabbene, F. & Tempo, R. (2011). Survey paper: research on probabilistic methods for control system design. *Automatica Journal of IFAC,* 47(7), 1279-1293.

Campbell, D. (2005). *E-commerce and the law of digital*. London: Oxford University Publishers.

Cassim, F. (2012). Addressing the spectre of cyber terrorism: a comparative perspective. *Potchefstroom Electronic Law Journal,* 15(2), 380-415.

Ceccagnoli, M., Forman, C., Huang, P. & Wu, D.J. (2012). Cocreation of value in a platform ecosystem: the case of enterprise software. *MIS Quarterly,* 36(1), 363-290.

Cecere, G. & Rochelandet, F. (2013). Privacy intrusiveness and web audiences: empirical evidence. *Telecommunications Policy, 37(10*), 1004-1014.

Chahar, C., Chauhan, V. & Das, M. (2012). Code analysis for software and system security using open source tools. *Information Security Journal: A Global Perspective*, 21(6), 346-352.

Chambers-Jones, C. (2013). Policing cyber hate, cyber threat and cyber terrorism. *International Journal of Police Sciences & Management,* 15(1), 74-75.

Chance-Hill, A., & Odell, N. (2014). Aiming to boost ecommerce. *Journal of Multidisciplinary Research, 3(2), 11-22.*

Charlesworth, A. & Pearson, S. (2013). Developing accountability-based solutions for date privacy in the cloud. *Innovation: the European Journal of Social Sciences,* 26(1/2), 7-35.

Chia, K. (2005). Singapore. In: Campbell, D. (ed) *E-commerce and the law of digital*. London: Oxford University Publishers.

Coetzee, R.V. (1999). A conceptual model for the functional integration of configuration management principles in corporate data management. Thesis submitted in fulfilment of the requirements for the degree Philosphiae Doctor at the Post-Graduate School for Management, Potchefstroom University for Christian Higher Education.

Collan, M., Fedrizzi, M. & Luukka, P. (2013). A multi-expert system for ranking patents: an approach based on fuzzy pay-off distributions and a TOPSIS-AHP framework. *Expert Systems with Applications: An International Journal*, 40(12), 4749-4759.

Collin, S. (1998). *Doing business on the Internet*. London: Kogan Page.

Corrado, I.S. (2013). Evaluating e-commerce websites cognitive efficiency: an integrative framework based on data environment analysis. *Applied Ergonomics,* 44(6), 1004-1014.

Costante, E., Paci, F., & Zannone, N. (2013). *Privacy-aware web service composition and ranking. International Journal of web services research, 10(3), 1-23.*

Cox, J. (2012). Information systems user: a structured model of the knowing-doing gap. *Computers in Human Behaviour,* 28(5), 1849-1858.

Cresswell, J.W. (2007). Qualitative inquiry and research design: choosing among five approaches. Sage Publications: London.

Crume, J. (2000). *Inside Internet security: what hackers don't want you to know.* New York: Addison-Wesley.

Dagada, R. & Eloff, M.M. (2013). Integration of policy aspects into information security issues in South African organisations. *African Journal of Business Management,* 7(31), 3069-3077.

Dagada, R. & Mukwevho, S. (2013). Industrial Espionage Threats in Corporate South Africa. *Proceedings of the Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensics* (CyberSec2013), the Asia Pacific University of Technology and Innovation, March 4-6 2013, 162-169.

Dagada, R. (2013). Digital Banking security, Risk and Credibility Concerns in South Africa. *Proceedings of the Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensics* (CyberSec2013), the Asia Pacific University of Technology and Innovation, March 4-6 2013, 148-161.

Dagada, R., Eloff, M.M. & Venter, L.M. (2009). Too many laws but very little progress! Is South African highly acclaimed information security legislation redundant? *ISSA 2009 Conference*. University of Johannesburg, 6 to 8 July 2009.

De Guinea, A.O., Titah, R. & Leger, P.M. (2013). Measure for measure: a two study multi-trait multi-method investigation of construct validity in IS research. *Computers in Human Behaviour,* 29(3), 833-844.

De Kare-Silver, M. (2001). *E-shock: the new rules – Internet strategies for retailers and manufacturers.* New York: Amacom.

Derrida, J. (1997) Deconstruction in a nutshell: A conversation with Jaques Derrida /edited with a commentary by John D. Caputo. New York: Fordham University Press, 1997.

De Wet, C. & Du Plessis, R. (2004). Taxation (VAT) In: Buys R. & Cronjé, F. (eds.) (2004). *Cyberlaw: the Law of the Internet in South Africa*. Pretoria: Van Schaik Publishers, 276-294.

Deane, J.K., Ragsdale, C.T., Rakes, T.R. & Rees, L.P. (2009). Managing supply chain risk and disruption from IT security incidents. *Operations Management Research,* 2(1-4), 4-12.

Demirhan, E. & Dermirtas, G. (2011). Do the advances in information technologies complicate the conduct of monetary policy? *Ataturk University Journal of Economics & Administrative Sciences,* 25(3/4), 1-12.

Demirkan, H. & Delen, D. (2013). Leveraging the capabilities of service-oriented decision support system: putting analytics and big data in cloud. *Decision Support Systems,* 55(1), 412-421.

Dixit, D.K. (2013). Contribution of educational psychology and methods of research in education. *Indian Streams Research Journal,* 3(9), 1-5.

Dolcil, P.C., Macadall, A.C.G. (2014). Information technology investments and supply chain governance. *RAC, 18(2), 217-235.*

Drabble, S.J., & O'Cathan, A. (2014). Describing qualitative research undertaken with randomised controlled trials in grant proposals: a documentary analysis. *BMC Medical Research Methodology, 14(1), 1-17.*

Dunlop, A.J.S. (2005). South Africa. In: Campbell, D. (ed.). *E-commerce and the Law of Digital Signatures*. Dobbs Ferry, NY: Oceana, 559-578.

Elmalech, A., & Sarne, D. (2014). Evaluating the applicability of peer-designed agents for mechanism evaluation. *Web Intelligent & Agent Systems, 12(2), 171-191.*

Fang, Y., & Qureshi, I. (2014). Trust, satisfaction, and online repurchase intention: the moderating role of perceived effectiveness of e-commerce institutional mechanisms. *MIS Quarterly,* 38(2), 407-438.

Fatt, E.K. & Wahjanto, A. (2005). Malaysia. In: Campbell, D. (ed.). *E-commerce and the Law of Digital Signatures*. Dobbs Ferry, NY: Oceana, 427-448.

Feng, B., Ma, J. & Fan, Z.P. (2011). An integrated method for collaborative R & D project selection: supporting innovative research teams. *Expert Systems with Applications: An International Journal,* 38(5), 5532-5543.

Flanagin, A., & Metzger, M.J. (2014). Mitigating risk in ecommerce transactions: perceptions of information credibility and the role of user-generated ratings in product quality and purchase intention. *Journal Electronic Commerce Research, 14(1), 1-23.*

Gabrys, E. (2004) The international dimensions of Cyber-crime. In: Tipton, H. F. and Krause, M. (eds.) *Information security management handbook*. London: Auerbach Publications, pp 1823-1839.

Ginn, J. (2013). Cyber crime. *Capitol Ideas,* 56(4), 12-15.

Goel, S. & Shawky, H.A. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management,* 46(7), 404-410.

Goncalves, M.E., & Jesus, I.A. (2013). Security policies and the weakening of personal data protection in the European Union. *Computer Law & Security Review, 29(3), 255-263.*

Goo, J., & Yim, M.S. (2014). A path to successful management of employee security compliance: an empirical study of information security climate. *IEEE Transactions on Professional Communication, 57(4), 286-308.*

Griffiths, D.H. & Harrison, J. (2005). United Kingdom. In: Campbell, D (ed.). *E-commerce and the law of digital signatures.* Dobbs Ferry, NY: Oceana, pp 151-174.

Groenewald, M. (2000). Towards an electronic commerce for South Africa. In: Buys, R. (ed.) *Cyberlaw: the Law of the Internet in South Africa*. Pretoria: Van Schaik Publishers, 97-112.

Gupta, M. & Narain, R. (2012). A study on usage of IT and its implications on e-procurement in Indian organisations. *International Journal of Business Information Systems,* 10(2), 222-244.

Gupta, M., Jin, S., Sanders, G.L., Sherman, B.A. & Simha, A. (2012). Getting real about virtual worlds: a review. *International Journal of Virtual Communities and Social Networking,* 4(3), 1-46.

Haar, A., Norlyk, A., & Hall, E.O.C. (2014). Ethical challenge embedded in qualitative research interviews with close relatives. *Nursing Ethics, 21(1), 6-15.*

Hamadouche, S., & Lanet, J.L. (2013). Virus in a smart card: myth or reality. *Journal of Information Security and Applications, 18(3), 130-137.*

Hanser, R.D. (2011). Gang-related cyber and computer crimes: legal aspects and practical points of consideration in investigations. *International Review of Law, Computers and Technology – Crime and CriminalJjustice,* 25(1-2), 47-55.

Hare, C. (2004). Policy development. In: Tipton, H.F. & Krause, M. (eds.). *Information Security Management Handbook*. London Auerbach Publications, 925-944.

Hassan, D. & Sabry, A. (2013). Encoding secure information flow with restricted delegation and revocation in Haskell. *Proceedings of the 1st Annual Workshop on Functional Programming Concepts in Domain-specific Languages*, 11-18.

Henning, E., Van Rensburg, W. & Smit, B. (2004). *Finding your way in qualitative research*. Pretoria: Van Schaik Publishers.

Herman, B.D. (2012). Taking the copyfight online: comparing the copyright debate in congressional hearings, in newspapers, and on the web. *Journal of Computer-mediated Communication,* 17(3), 354-368.

Hilmi, M.F., Pawanchik, S., Mustapha, Y. & Ali, H.M. (2013). Information security perspective of a learning management system: an exploratory study. *International Journal of Knowledge Society Research,* 4(2), 9-10.

Huey, L., Nhan, J. & Broll, R. (2013). 'Uppity civilians' and 'cyber-vigilantes': The role of the general public in policing cyber-crime. *Criminology & Criminal Justice: An International Journal,* 13(1), 81-97.

Ioannidis, C., Pym, D. & Williams, J. (2012). Information security trade-offs and optimal patching policies. *European Journal of Operational Research,* 216(2), 434-444.

Issacs, L. (2013). Rolling the dice with predictive coding leveraging analytics technology for information governance. *Information Management Journal,* 47(1), 22-26.

Jairak, R. & Praneetpolgrang, P. (2013). A practical approach for improving B2C e-commerce services with a trust capability maturity model. *International Journal of e-Services and Mobile Applications,* 5(2), 22-36.

James, S., & Rajendran, L. (2013). Effect of public relation on customer loyalty with special reference to ecommerce portals. *Journal of Multidisciplinary Research,* 5(2), 87-102.

James, T., Nottingham, Q., & Kim, B. (2013). Determining the antecedents of digital security practices in the general public dimension. *Information technology & management,* 14(2), 69-89.

Jirasek, V. (2012). Practical application of information security models. *Information security technical report,* 17(1-2), 1-8.

Joshi, A, Salaria, T & Naidu, G. (2005). India. In: Campbell, D (ed.) E-commerce and the law of digital signatures. Dobbs Ferry, NY: Oceana, pp 289-327).

Julisch, K. (2013). Understanding and overcoming cyber security anti-patterns. *Computer Networks: the International Journal of Computer and Telecommunications Networking*, 57(10), 2206-2211.

Junio, T.J. (2013). How probable is cyber war? Bringing IR theory back in the cyber crime debate. *Journal of Strategic Studies,* 36(1), 125-133.

Kalmbach, J. (2013). The invisible and the need for new research methodologies. *Communication Design Quarterly Review,* 1(4), 26-28.

Kalra, S., & Sood, S. (2013). Advanced remote authentication protocol for multi-server architecture based ECC. *Journal of Information Security and Applications, 18(3), 98-107.*

Kamel, N., & Lanet, J.L. (2013). Risks induced by web applications on smart cards. *Journal of Information Security and Applications, 18(3), 148-156.*

Kauffman, R.J., Techata, A.A. & Wang, B. (2012). Event history, spatial analysis and count data methods for empirical research in information systems. *Information Technology and Management,* 13(3), 115-157.

Kehe, W. & Shichao, Y. (2014). An information security threat assessment based on Bayesian network and OWA operator. *Applied Mathematics & Information Sciences,* 8(2), 833-838.

King Report on Governance for South Africa (2002). Johannesburg: Institute of Directors Southern Africa.

King Report on Governance for South Africa (2009). Johannesburg: Institute of Directors Southern Africa.

King, M. & Lessidrenska, T. (2009). *Transient caretakers: Making Life on Earth Sustainable.* Johannesburg: Pan Macmillan.

Klimova, S.G. & Mikheyenkova, M.A. (2012). Formal methods of situational analysis: experience from their use. *Automatic Documentation and Mathematical Linguistics,* 46(5), 183-194.

Koskosas, I.V. (2012). Cultural and organisational commitment in the context of e-banking. *International Journal of Internet Technology and Secured Transactions,* 4(1), 26-41.

Krause, M. (2004). Ethics and the Internet In: Tipton, H.F. & Krause, M. (Eds) (2004). *Information Security Management Handbook.* London: Auerbach Publications, 1911-1920.

Kshetri, N. (2013). Privacy and security issues in cloud computing: the role of institutions and institutional evolution. *Telecommunications Policy,* 37(4-5), 372-386.

Kuo, Y. & Fan, H.L. (2005). Taiwan. In: Campbell, D. (ed.). *E-commerce and the Law of Digital Signatures*. Dobbs Ferry, NY: Oceana, 619-636.

Kwuida, L. & Schmidt, S.E. (2011). Valuations and closure operators on finite lattices. *Discrete Applied Mathematics*, 159(10), 990-1001.

Lai, Y.L. (2013). Analyzing strategies of mobile aganets on malicious cloud platform with agent-based computational economic approach. *Expert Systems with Applications,* 40(7), 2615-2620.

Latimer, P. (2013). How to ensure disclosure of information in securities markets post-GFC. *Common Law World Review,* 42(2), 111-136.

Lautenbach, G.V. (2005). Lecturers' changing epistemologies and pedagogies during engagement with Information and Communication Technology in an education faculty. Thesis submitted in fulfilment of the requirements for the degree Doctor Educationis in Computer-based Education in the Faculty of Education at the University of Johannesburg.

Lawande, P.P. (2012). A study of effectiveness of cyber laws in dealing with cyber crimes in developing country like India. *Golden Research Thoughts,* 2(1), 1-9.

Lawrence, E. Corbitt, B. Fisher, J. Lawrence, J. & Tidwell, A. (2000). *Internet commerce: digital models for business.* New York: John Wiley & Sons.

Lee, K.J. (2012). The coevolution of IT innovation and copyright institutions: the development of the mobile music business in Japan and Korea. *The Journal of Strategic Information Systems,* 21(3), 245-255.

Leverich, BB; Gallagher-Duff, KT; Lavelleye, MA & Rosette, K (2003) Trademarks. In: Li, C., Peters, G.F., Richardson, V.J. & Watson, M.W. The consequences of information technology control weaknesses on management information systems: the case of Sarbanes-Oxley internal control reports. *MIS Quarterly,* 36(1), 179-204.

Li, J.S., Zhang, X.G., Chu, J., Suzuki, M. & Araki, K. (2012). Design and development of EMR supporting medical process management. *Journal of Medical Systems*, 36(3), 1193-1203.

Lin, H. (2012). A virtual necessity: some modest steps toward greater cybersecurity. *Bulletin of the Atomic Scientist*, 68(5), 750-87.

Liu, G. (2013). Visualization of patents and papers in terahertz: a comparative study. *Scientometrics,* 94(3), 1037-1056.

Loblich, M. & Wendelin, M. (2012). ICT policy activism on a rational level: ideas, resources and strategies of German civil society in governance processes. *New Media & Society,* 14(6), 899-915.

Loebl, Z. (2005). Czech Republic. In: Campbell, D (ed.) *E-commerce and the Law of Digital Signatures*. Dobbs Ferry, NY: Oceana, 89-202.

Lostorto, C. (2013). Evaluating ecommerce websites cognitive efficiency: an integrative framework based on data envelopment analysis. *Applied ergonomics, 44(6), 1004*-1014.

Lu, B. (2013). Reconstructing copyright from 'copy-centric' to 'dissemination-centric' in the digital age. *Journal of Information Science,* 39(4), 479-493.

Luyinda, R., Herselman, M.E. & Botha, G.H.K. (2008). IT control objectives for implementing the Public Management Act in South Africa. *Issues in Information Science & Information Technology,* 5(3), 29-49.

Ma, L. (2012). Some philosophical considerations in using mixed methods in library and information science research. *Journal of the American Society for Information Science and Technology*, 63(9), 1859-1867.

Mahadeo, D.V. & Shivaji, W.M. (2013). A survey on awareness of cyber crime related issues with reference to citizens of Baramati region. *Indian Streams Research Journal,* 3(3), 1-15.

Maiwald, E. (2004) *Fundamentals of Network Security*. New York: McGraw-Hill

Makinen, S. (2013). Some records manager will take care of it – records management in the context of mobile work. *Journal of Information Science,* 39(3), 384-396.

Mamaghan, N.D., Madani, F.M. & Sharifi, A. (2012). Customer oriented enterprise IT architecture framework. *Telematics and Informatics,* 29(2), 219-232.

Martin, A.K. & De Andrade, N.N.G. (2013). Friending the taxman: on the use of social networking services for government elD in Europe. *Telecommunications Policy.* 37(9), 715-724.

Masete, N.T. (2012). The challenges in safeguarding financial privacy in South Africa. *Journal of International Commercial Law &Technology,* 7(3), 248-259.

Maskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centred information security: managing a strategic balance between prevention and response. *Information and Management, 51(1), 138-151.*

Maswera, T., Edwards, J. & Dawson, R. (2012). Recommendations for e-commerce systems in the tourism industry of sub-Saharan Africa. *Telematics and Informatics,* 26(1), 1 2-19.

Mathiesen, M. (1997). *Marketing on the Internet: a proven 12-step plan for promoting, selling, and deliveringyour products and services to millions over the information superhighway*. Gulf Breeze: Maximum Press.

Mbaku, J.M. & Yu, Z. (2013). Information communication technologies transparency and governance in China. *International Journal on World Peace*, 30(1), 9-59.

McGraw, G. (2013). Cyber war is inevitable. *Journal of Strategic Studies,* 36(1), 109-119.

McLaughlin, C.G., Devers, K.J. (2012). Obtaining providers 'buy-in' and establishing effective means of information exchange will be critical to HITECHs' success. *Health Affairs,* 31(3), 514-526.

Merriam, S.B. (1998). *Qualitative Research & Case Study Applications in Education*. San Francisco: Jossey-Bass Publishers.

Miller, W.L., Crabtree, B.F., Harrison, M.I. & Fennell, M.L. (2013). Integrating mixed methods in health services and delivery system research. *Health Services Research,* 48(6), 2125-2133.

Mitropoulos, S., Othonos, C. & Douligeris, C. (2013). An effective and secure web banking system: development and evaluation. *International Journal of Business Information Systems,* 12(3), 335-361.

Mohite, B.J. & Kumthekar, D.M. (2013). Awareness of IT security laws and security maintenance policies: two pillars of information security management. *Golden Research Thoughts,* 2(7), 1-6.

Moore, T., Clayton, R. & Anderson, R. (2009). The economics of online crime. *Journal of Economics Perspectives,* 23(3), 3-20.

Morrison, M.I. (2013). The acquisition supply chain and the security of government information technology purchases. *Public Contract Law Journal,* 42(4), 749-749.

Moschovitis, C.J.P., Poole, H., Schuyler & Senft. T.M. (1999). *History of the Internet: a chronology, 1843 to the present*. Santa Barbara: ABC-CLIO.

Mouton, J. (2001). *How to succeed in your masters and doctoral studies: a South African guide and resource book.* Pretoria: Van Schaik Publishers.

Mukundan, N.R. & Sai, L.P. (2014). Perceived information security of internal users in Indian IT services industry. *Information Technology and Management, 15(1), 1-8.*

Mukwevho, H.S. (2010). Industrial espionage in corporate South Africa. A research report submitted to the Faculty of Commerce, Law, and Management, University of the Witwatersrand, in fulfillment of the requirements for the degree of the Master of Management (in the field of Public and Development Management).

Naimark, Y.I. & Teklina, L.G. (2011). Possibilities of using pattern recognition methods in research on mathematical models. *Pattern Recognition and Image Analysis,* 21(2), 195-198.

Nanevski, A., Banerjee, A. & Garg, D. (2013). Dependant type theory for verification of information flow and access control policies. *ACM Transactions on Programming Languages and Systems,* 35(2).

Navarra, D.D. (2013). Perspectives on the evaluation of geo-ICT for sustainable urban governance: implications for e-government policy. *Journal of the Urban & Regional Information Systems Association*, 25(1), 19-28.

Nehinbe, J.I.O. (2012). A comparative study of attributes for gathering admissible evidence in the investigation of distributed denial of service (DDoD) attacks. *International Journal of Internet Technology and Secured Transactions,* 4(2/3), 121-138.

Newington, L., & Metcalfe, A. (2014). Factors influencing recruitment to research: qualitative study of the experiences and perceptions of research team. *BMC Medical Research Methodology, 14(1), 1-20.*

Ngobeni, W., Lubisi, D. & Mahlangu, D. (2005). ANC boss probed for subversion. *Sunday Times,* 04 December 2005. Johannesburg: Johnic Communications.

Nichols-Hess, A., & LaPorte-Fiori, R. (2015). Preserving patron privacy in the 21st Century Academic Library. *Journal of Academic Librarianship, 41(1), 105-114.*

Nikolayevich, L.A., & Borisovna, P.N. (2014). Information-psychological security of a person: philosophical aspect. *Philosophy, History, Culture, 1(2), 1-7.*

Niu, J., & Reith, M. (2014). Formal verification of security properties in trust management policy. *Journal of Computer Security, 22(1), 69-153.*

Nye, J.S. (2013). From bombs to bytes: can our nuclear history inform our cyber future? *Bulletin of the Atomic Scientists,* 69(5), 8-14.

Overill, R.E. (2013). The ‘inverse CSI effect’: further evidence from e-crime data. *International Journal of Electronic Security and Digital Forensics*, 5(2), 81-89.

Panton, B.C., Colombi, J.M. Grimaila, M.R., & Mills, R,F. (2014). Strengthening DoD cyber with the vulnerability market. *Defense acquisition research Journal, 21(1), 465-484.*

Pardo, C., Pino, F.J., Garcia, F., Baldassarre, M.T., & Piattini, M. (2013). From chaos to the systematic harmonisation of multiple reference models: a harmonization framework applied in two case studies. *Journal of Systems and Software*, 86(1), 125-143.

Paterson, H. (2012). Stuck in the middle: the need to refine intermediary liability for copyright infringement in the P2P file-sharing world. *International Journal of Technology Policy and Law,* 1(1), 92-115.

Pellot, B. (2013). Hope on the horizon? *Index on Censorship,* 42(2), 23-27.

Pisaric, M. (2013). The normative response to problems of detection and investigation of cyber crime. *Proceedings of Novi Sad Faculty of Law,* 47(1), 291-307.

Pluye, P., Grad, R.M. & Johnson-Lafleur, J. (2013). Number needed to benefit from information: proposal from a mixed methods research study with practicing family physicians. *Annals of Family Medicine,* 11(6), 559-567.

Porrini, R., Palmonari, M., & Vizzari, G. (2014). Composite match autocompletion: a sematic result-oriented automation technique for e-marketplaces. *Web Intelligence & Agent Systems, 12(1), 35-49*.

Pozon, A.E.C. (2013). Cyber warfare: the effects of technological advancements in expanding the concept of war and the role of non-state actors and individuals. *Atejneo Law Journal,* 57(4), 1065-1082.

Proff, S. & Dettmann, A. (2013). Inventor collaboration over distance: a comparison of academic and corporate patents. *Scientometrics,* 94(3), 1217-1238.

Radha, T.G. & Mimal, K.M. (2012). Information and dynamice of SEIR e-epiodemic model for the spreading behaviour of malicious objects in computer network. *International Journal of Engineering Science & Technology,* 4(10), 4275-4282.

Rahman, H. & Ramos, I. (2013). Implementation of e-commerce at the grass roots: issues of challenging in terms of human-computer interactions. *International Journal of Information Communication Technologies and Human Development,* 5(2), 1-19.

Rantao, J. (2004). Sleep easy - but with one eye open. *The Star*, 6 August 2004. Johannesburg: Independent Newspapers.

Republic of South Africa (2008). *Companies Act No. 71 of 2008*. Cape Town: Government Printer.

Republic of South Africa (1996). *Constitution of the Republic of South Africa No. 108 of 1996.* Cape Town: Government Printer.

Republic of South Africa (2008). *Consumer Protection Act, No. 68 of 2008*. Cape Town: Government Printer.

Republic of South Africa (1978). *Copyright Act, No. 98 of 1978*. Cape Town: Government Printer.

Republic of South Africa (1993). *Designs Act No. 195 of 1993.* Cape Town: Government Printer.

Republic of South Africa (2005). *Electronic Communications and Transactions Act No. 25 of 2005.* Cape Town: Government Printer.

Republic of South Africa (1996). *Films and Publications Act No. 65 of 1996*. Cape Town: Government Printer.

Republic of South Africa (1997*). Intellectual Property Laws Amendment Act, No. 38 of 1997.* Cape Town: Government Printer.

Republic of South Africa (2008). *Intellectual Property Rights from Publicly Financed Research and Development Act No. 52 of 2008*. Cape Town: Government Printer.

Republic of South Africa (1995). *Labour Relations Act No. 66 of 1995*. Cape Town: Government Printer.

Republic of South Africa (1941). *Merchandise Marks Act, No. 17 of 1941*. Cape Town: Government Printer.

Republic of South Africa (1996). *National Archives and Records Service of South Africa Act No. 43 of 1996*. Cape Town: Government Printer.

Republic of South Africa (2005). *National Credit Act No. 34 of 2005*. Cape Town: Government Printer.

Republic of South Africa (1978). *Patents Act No. 57 of 1978*. Cape Town: Government Printer.

Republic of South Africa (1967). *Performers' Protection Act No. 11 of 1967*. Cape Town: Government Printer.

Republic of South Africa (2000). *Promotion of Access to Information Act No. 2 of 2000*. Cape Town: Government Printer.

Republic of South Africa (2013). *Promotion of Personal Information Act, 4 of 2013*. Cape Town: Government Printer.

Republic of South Africa (2009). *Protection of Personal Information Bill No. 9 of 2009*. Cape Town: Government Printer.

Republic of South Africa (2002*), Regulation of Interception of Communications and Provision of Communication-related Act No. 70 2002*. Cape Town: Government Printer.

Republic of South Africa (1993). *Trade Marks Act No. 194 of 1993*. Cape Town: Government Printer.

Richardson, P.S. (2000). Internet marketing: readings and online resources.
New York: McGraw - Hill

Rogerson, K. & Milton, D. (2013). A policymaking process "Tug-of-War": National information security policies in comparative perspective. *Journal of Information Technology & Politics,* 10(4), 462-476.

Roman, R., Zhou, J. & Lopez, J. (2013). On the features and challenges of security and privacy in distributed Internet of things. *Computer Networks: International Journal of Computer and Telecommunications Networking,* 57(10), 2266-2279.

Ruggiano, N. & Brown, E.L. (2013). Adding home health care to the discussion on health information technology policy. *Home Health Care Services Quarterly,* 32(3), 149-162.

Saeedi, A. & Doolen, T. (2012). A computer-assisted qualitative data analysis framework for the engineering management domain. *International Journal of Data Analysis Techniques and Strategies,* 4(1), 1-20.

Salzberg, C.A. & Jang, Y. (2012). Policy initiative for health information technology: a qualitative study of U.S. expectations and Canada's experience. *International Journal of Medical Informatics,* 81(10), 713-722.

Sanchez-Pena, J.J., & Fernandez-Vicente, E. (2013). ITIL, COBIT and EFQM: can they work together? *International Journal of Combinatorial Optimization Problems & Informatics,* 4(1), 54-64.

Saunders, C.S. & Wu, Y.A. (2011). Governing information security: governance domains and decision rights allocation patterns. *Information Resources Management Journal*, 24(1), 28-45.

Scammon, D.L., Tamoaia-Cotisel, A., Day, R.L. & Day, J. (2013). Connecting the dots and merging meaning: using mixed methods to study primary care delivery transformation. *Health Services Research*, 48(6), 2181-2207.

Schneider, F.B. (2000). Enforcement security policies. *ACM Transactions on Information and Systems Security*, 3(1), 30-50.

Schneier, B. (2000). *Secrets and lies: digital security in a networked world.* New York: John Wiley & Sons.

Schneier, B. (2003). Attack trends. *Queue*, 3(5), 52-53.

Schonwetter, T., Ncube, C., & Chetty, P. (2010). South Africa. In: Armstrong, C., De Beer, J. Kawooya, D., Prabhala, A., & Schonwetter, T. (eds.). *Access to knowledge in Africa: the role of copyright.* Cape Town: UCT Press. 231-280.

Serrano, E., Rovatsos, M. & Botia, J.A. (2013). Data mining agent conversations: a qualitative approach to multi-agent systems analysis. *Information Sciences: International Journal,* 230(15), 132-146.

Sharifi, A. & Tripunitara, M.V. (2013). Least-restrictive enforcement of the Chinese wall security policy. *SACMAT '13 Proceedings of the 18th ACM Symposium on Access Control Models and Technologies,* 61-72.

Shipps, B. & Phillips, B. (2013). Social networks, interactivity and satisfaction: assessing socio-technical behavioural factors as an extension to technology acceptance. *Journal of Theoretical and Applied Electronic Commerce Research, 8(1), 35-52.*

Shu'aibu, B. & Sukri, M. (2013). Modelling the determinants of ICTs policy formulation in technical and vocational education in Nigerian institute of higher learning. *Indian Journal of Science & Technology,* 6(4), 4273-4281.

Silva, L. & Fulk, H.K. (2012). From disruptions to struggles: theorizing power in ERP implementation projects. *Information & Organisation,* 22(4), 227-251.

Simon, D.A (2013). The confusion trap: rethinking parody in trademark law. *Washington Law Review,* 88(3), 1021-1101.

Simmonds, V.W., & Christopher, S. (2013). Adapting western research methods to indigenous ways of knowing. *American Journal of Public Health,* 103(12), 2185-2192.

Singh, S. (2010). The South African 'information society', 1994-2008: problems with policy, legislation, rhetoric and implementation. *Journal of Southern African Studies*, 36(1), 209-227.

Singh, Y.N. & Singh, S.K. (2013). A taxonomy of biometric system vulnerabilities and defences. *International Journal of Biometrics*, 5(2), 137-159.

Siponen, M., Mahmood, M.A., & Pahnila, S. (2014). Employee's adherence to information security policies: an exploratory field of study. *Information and Management, 15(2), 217-224.*

Skoudis, E. (2004). A new breed of hacker tools and defences. In: Tipton, H.F., & Krause, M. (eds.). *Information Security Management Handbook.* London: Auerbach Publications, 135-146.

Slade, R.M. (2004). Malware and computer viruses. In: Tipton, H.F. & Krause, M. (eds.). *Information Security Management Handbook*. London: Auerbach Publications, 1257-1286.

Sole, S. & Letsoalo, M. (2005). How Kasrils trapped Masetlha. *Mail & Guardian*, 18 November 2005. Johannesburg: M&G Media Ltd.

Sood, A.K. & Enbody, R. (2013). Targeted cyber-attacks: a superset of advanced persistent threats. *IEEE Security and Privacy,* 11(1), 54-61.

Sowan, A.K. & Jenkins, L.S. (2013). Use of the seven principles of effective teaching to design and deliver an interactive hybrid nursing research course. *Nursing Education Perspectives,* 34(5), 315-322.

Stampler, L. (2013). China's countless lonely hearts turn to retail theraphy on singles' day, break ecommerce records. *Journal of Multidisciplinary Research, 4(2), 78-89.*

Stantchev, V., Petruch, K. & Tamm, G. (2013). Assessing and governing IT staff behavior by performance-based simulation. *Computers in Human Behaviour*, 29(2), 473-485.

Stephanou, A. (2008). *The impact of information security awareness training on information security behaviour.* A research report submitted to the Faculty of Commerce, Law and Management, University of the Witwatersrand, in partial fulfilment of the requirements for the degree of Master of Commerce. Johannesburg: University of the Witwatersrand.

Stephanou, T. & Dagada, R. (2009). The impact of information security awareness training on information security behaviour: the case of further research. *ISSA 2008 Conference*. University of Johannesburg, 2 to 4 July 2008.

Stone, J. (2013). Cyber war will take place! *Journal of Strategic Studies,* 36(1), 101-108.

Strang, K.D. (2013). Risk management research design ideologies, strategies, methods and techniques. *International Journal of Risk and Contingency Management,* 2(2), 1-26.

Szeman, P. (2005). Hungary. In: Campbell, D. (ed.). *E-commerce and the law of digital signatures*. Dobbs Ferry, NY: Oceana, 269-285.

Thaanum, J.D. (2013). Threats to cyber security: the dangers of malicious mobile code, users, and the iPhone. *Journal of Applied Security Research,* 18(4), 490-509.

Thompson, D.R. (2014). Teaching RFID information systems security. *IEEE Transactions on Education, 57(1), 42-47.*

Ting, C. & Yi, F. (2013). ICT policy for the “socialist new countryside” – a case study of rural informatization in Guangdong, China. *Telecommunications Policy,* 37(8), 626-638.

Tiwari, B.K. (2013). Cyber crimes and its jurisdiction. *Indian Streams Research Journal,* 3(5), 1-5.

Trope, R.L. & Humes, S.J. (2013). By executive order: delivery of cyber intelligence imparts cyber responsibilities. *IEEE Security and Privacy,* 11(2), 63-67.

Tsolis, D.K., Tsolis, G.K., Karatzas, E.G. & Papatheodorou, T.S. (2002). Copyright protection and management and a web-based library for digital images of the Hellenic cultural heritage. *Proceedings of the 2001 Conference on Virtual Reality, Archeology, and Cultural Heritage*, 53-60.

United States of America. (2002). Sarbanes-Oxley Act of 2002. Washington DC.

Van Niekerk, J. & von Solms, R. (2004). Organisational learning models for information security. *Peer-reviewed Proceedings of the ISSA 2004: Enabling Tomorrow Conference,* 30 June – 2 July, Gallagher Estate, Midrand.

Vijaya, K.M. (2013). Cryptography – a solution for information security threats. *Golden Research Thoughts,* 3(1), 1-3.

Warren, M.J. & Leitch, S. (2010). Critical supply chain systems and critical infrastructure protection. *International Journal of Logistics Economics and Globalisation*, 2(2), 107-117.

Washah, S. (2013). E-commerce perception within small business of minority communities. *International Journal of Technology, 9(3), 49-62*.

Weiser, S.M. (2005). United States. In: Campbell, D. (ed.). *E-commerce and the Law of Digital Signatures*. Dobbs Ferry, NY: Oceana, 695-732.

Welman, J.C. & Kruger, S. (2001). *Research methodology for the business and administrative Sciences*. Cape Town: Oxford University Press Southern Africa.

Westby, J.R. (2013). Cybersecurity & law firms: a business risk. *Law Practice: the Business of Practicing Law,* 39(4), 46-49.

Williams, C.K. & Karahanna, E. (2013). Causal explanation in the coordinating process: a critical realist case study of federated IT governance structures. *MIS Quarterly*, 37(3), 933-967.

Williams, P.A.H. (2013). Does the PCEHR mean a new paradigm for information security? Implications for health information management. *Health Information Management Journal,* 42(2), 31-36.

Wu, K., & Ye, S. (2014). An information security threat assessment model based on Bayesian network and OWEA operator. *Applied mathematics & information sciences, 8(2), 833-838.*

Wu, X. & Sun, W. (2013). Robust copyright protection scheme for digital images using overlapping DCT and SVD. *Applied Soft Computing*, 13(2), 1170-1182.

Wu, X. (2013). Shallow talk about information security in the corporate office. *Canadian Social Science,* 9(2), 34-39.

Xiong, C. (2013). Coexist, complement, converge and innovate: public diplomacy of US-China Internet industry forum. *Telematics and Informatics*, 30(4), 331-334.

Yaokumah, W. (2013). Evaluation of the effectiveness of information security governance practices in developing nations: a case of Ghana. *International Journal of IT / Business Alignment and Governance,* 4(1), 27-43.

Yoshikane, F. (2013). Multiple regression analysis of a patent’s citation frequency and quantitative characteristics: the case of Japanese patents. *Scientometrics,* 96(1), 365-379.

Zhang, Y., Zhang, D. & Mi, G. (2012). Research article: using ensemble methods to deal with imbalanced data predicting protein-protein interactions. *Computational Biology and Chemistry,* 36(4), 36-41.

Zinszer, K. & Tamblyn, R. (2013). A qualitative study of health information technology in the Canadian public health system. *BMC Public Health,* 13(1), 1-7.

Zissis, D. & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems,* 28(3), 583-592.

Rabelani Dagada is a PhD student at the University of South Africa and teaches Technology & Information Management at the Wits Business School of the University of the Witwatersrand, Johannesburg.

Professor Mariki Eloff is the Chief Researcher at the Institute for Corporate Citizenship, College of Economic and Management Sciences, University of South Africa.

APPENDICES

APPENDIX A1

REQUEST TO PARTICIPATE IN THE STUDY

<<Company>>
<<Respondent>>

Dear <<Surname>>

I am a Lecturer of Information and Communications Technology (ICT) at the Wits Business School of the University of the Witwatersrand and I am currently completing PhD - Information Systems in the University of South Africa's School of Computing. The title of my research report is:

"Legal and policy aspects to consider when providing information security in the corporate environment"

As part of this study, I should interact with at least 40 South African companies and other organisations that are using their websites to conduct financial transactions between themselves and their customers as part of trading. It is on this ground that I hereby request a meeting with you during the day and time convenient to you. You may also be asked to consent to being interviewed and having this interview tape-recorded for data analysis. These tape recorded interviews will be coded (using pseudonyms) and be stored in a locked facility.

Please note that if you agree to be part of this study you are at liberty to withdraw from the study at any time, without any pressure to provide reasons. I also undertake all possible means to ensure that your career and/or organisation is not caused any detriment by partaking in this study and I will accordingly allocate a pseudonym to all participants to protect their identity and to guarantee that any information revealed, either personal or professional, will be regarded as absolutely confidential.

In addition, it is my belief that there are number of possible benefits for you and/or your organisation as a participant in this study. On the completion of the study I shall supply you with a bound copy of the final, approved research report. I may also provide a short presentation on the findings to you and some of your colleagues. You will also receive conference papers and published articles with regard to this research. The study will also expose you to a host of literature from a variety of sources and reflecting on your own growth as an information security practitioner could be beneficial in your professional development.

I am doing this study under the supervision of Professor Mariki Eloff. Please feel free to contact them regarding this study if you deem it necessary. Their contact details as follows:

Supervisor:	Prof Mariki Eloff
Institution:	University of South Africa
Division:	School of Computing
Tel:	012 429 6336
Email:	eloffmm@unisa.ac.za

I would very much appreciate your assistance.

Yours sincerely,

[By email]
Rabelani Dagada

Tel: 073 2140 174 or 011 717 7162
Email: Rabelani.Dagada@wits.ac.za

APPENDIX A2

PROFILES OF THE ORGANISATIONS THAT PARTICIPATED IN THIS STUDY

Organisation 1

This organisation, listed on the Johannesburg Stock Exchange, is one of the largest banks in South Africa. The Group offers a complete suite of financial services and products, including banking, assurance and wealth management. Organisation 1 mainly operates in South Africa, but has equity holdings in other banks in Mozambique and Tanzania. This bank has representative offices in Namibia and Nigeria. It had, by 31 December 2010, assets of R716,5 billion, 118 million customers, and 36 770 permanent employees. This bank was established in 1991 after the amalgamation of four South African banks. The Group was the first bank in South Africa to offer access to personal banking details online in October 1996 and by 1997 it made the first SET (Secure Electronic Transaction)-compliant transaction in South Africa with a customer buying a music album from the South African online music store, CDM. In February 1997, it became the first South African bank to conduct a trial project piloting Visa and MasterCard's Secure Electronic Transmissions standard. In August 2000, Organisation 1 announced the first mobile banking service in South Africa, in conjunction with a mobile network operator. In July 2003[20] this bank was the first in South Africa whose customers' online bank accounts were hacked and defrauded.

Organisation 2

Organisation 2 is a bank holding company with its main subsidiary being one of the South African big four banks. The bank is listed both in Johannesburg Stock Exchange and Namibian Stock Exchange. This bank offers a variety of wholesale and retail banking services, insurance, asset management, and wealth management. This is one of the oldest banks in South Africa having been established in 1831. It currently focuses on Southern Africa and was the first South African Bank to allow online transactions in February 1997.[21] The other three big banks only enabled its customers to access banking services online between March and July 1997.

Organisation 3

It was established in South Africa approximately 150 years ago. Organisation 3 is now one of the big four banks in South Africa and has become a considerable global player which operates in 17 African countries. It also has operations in 13 countries outside of the African continent, especially in emerging markets. This bank is listed in two Stock Exchanges and its assets are valued over R1 341 billion. By December 2010 it had 53 000 employees worldwide and its market capitalisation was R170 billion. ICT plays an important role in terms of communications, integration and operations in Organisation 3 since it has operations in various branches, towns, cities, provinces, and countries. Organisation 3 became the first bank in July 2003 to offer customers free anti-virus and personal firewall software. This bank has a dedicated team of information security specialists which operates 24 hours a day to combat cyber crimes. This team[22] removes spoofing websites within 48 hours after its creation and block some of the phishing emails before they reach the customer.

Organisation 4

Listed on the Johannesburg Stock Exchange, Organisation 4 is one of the biggest financial institutions in South Africa. The Group offers an assortment of financial services and products in South Africa,

[20] This information was obtained from the World Wide Worx's 2006 Online Banking In South Africa Report. The Report was compiled by Arthur Goldstuck.

[21] This information was obtained from the World Wide Worx's 2006 Online Banking In South Africa Report. The Report was compiled by Arthur Goldstuck.

[22] This information was obtained from the Draft Digital banking Report in South Africa authored by Arthur Goldstuck of the World Wide Worx and Rabelani Dagada of the Wits Business School.

Africa, and other international markets. There are three banks within the Group. The Group was originally founded in the 1970's as a specialist investment bank by three entrepreneurs. It was established in its current form in 1998 through the merger of some financial entities. Since then Organisation 4 has been growing through organic, acquisition and green fields approach. One of the banks within the Group was the first to provide online car finance in July 1997.

Organisation 5
The Group has approximately 6 716 employees in its operations in South Africa, the United Kingdom, and Australia. Since Organisation 5 was founded in 1974 in South Africa, it has grown substantially through both strategic organic and acquisitions. It has distinctive private bank and asset managers whose customers are a select middle and upper class client base. In July 2002, it became the first South African company to list in London and Johannesburg. This bank does not have branches and Automated Teller Machines and thus most of the banking transactions are conducted through the mobile and online delivery channels.

Organisation 6
This company was the first mobile telecommunications operator to function in South Africa. It is an international cellular network which operates in African countries such as Tanzania, Lesotho, Mozambique and the Democratic Republic of Congo. In or about August 2008, Organisation 6 acquired a certain network and satellite services company. The acquired company is a pan-African company and as such this transaction allowed Organisation 6 to operate in about 40 African countries. This would include being able to operate in Nigeria, which is arguably the biggest cellular phone market. This mobile operator's equity is largely owned by a British telecommunication behemoth, and minority shareholders in South Africa. The Group is the dominant mobile network in South Africa with an estimated market share of 58%. South Africa is the most profitable market in Africa. Organisation 6 was listed in the Johannesburg Stock Exchange on 17 May 2009. In August 2010, this mobile operator teamed up with one of the South African banking group to launch M-PESA money transfer service in South Africa. M-PESA enables consumers to transfer money via call phones.

Organisation 7
This is a South African-based online restaurant franchise chain where orders and financial transactions are done in the restaurant's website. Information security is very critical in this online restaurant franchise because there are three payment methods that can expose the customers to criminal elements if security is not tight – Credit Card, Electronic Funds Transfer (EFT), and EarthBucks. Credit Card payments are facilitated securely through Virtual Card Services. EFT payments enable the customer to place his/her order online and make transfer to the restaurant's bank account. EarthBucks is a saving account scheme – every time the customer place an order online, he/she earn EarthBucks. Once the order and payment are done, food is delivered to the customer's preferred delivery address.

Organisation 8
This franchise is possibly the world's biggest flower delivery service. It has a presence in 150 countries, including South Africa. Organisation 8 was founded in South Africa in 1950 and has more than 400 franchisees in South Africa and the rest of the African continent. Orders can be placed and paid online via a Credit Card. Customers are encouraged to buy online by giving them credits for conducting business in the website. The franchise' website also provides online gift vouchers and Virtual cards. Organisation 8 takes information security seriously and that is why its website is certified by Thawte. Once a payment has been made, delivery is done on a specified date and time. Contact details for conveying customer complaints are published on the website.

Organisation 9
Organisation 9 is the first low cost airline to operate in South Africa and is modelled as a "no frills" airline like those that operating other parts of the world such as Ryanair, Southwest and EasyJet. It was established in 2001 with the first flight between Johannesburg and Cape Town. Now it has several routes within South Africa and between South Africa and a few other countries in Southern

Africa. Other than enabling its customers to buy air tickets online, the website of Organisation 8 allows customers to browse, build, and procure cell phone packages online from the three cell phone network operators. Organisation 8 has won several awards based on independent surveys. ICT plays a fundamental role in this airline since most of its trading is done online and thousands of online financial transactions happen every day.

Organisation 10
This organisation is a low-cost airline headquartered in Kempton Park, South Africa. It started to operate in 2004 with three daily flights between OR Tambo and Cape Town Airports. It now operates in several South African airports and has flights between South Africa and Mozambique, Tanzania, and Zambia. Most air tickets are bought online and the airline has a "ticketless" boarding method where you only have to produce a proof of identity and reference number to check-in for the flight. Organisation 3 also has the "eCheck-In" which enables passengers to choose their seats before arriving at the airport. That is why ICT is very critical in this organisation.

Organisation 11
Organisation 11 was the latest Low Cost Airline to operate in South Africa. The airline was launched in October 2006. This low cost carrier enables its customers to buy the air tickets online. The airline encourages passengers to buy their air tickets online by giving them incentives (specials) which are only available in the website. Organisation 11 takes information security very seriously and thus its website is VeriSign Secured. This gives the customers who use Credits Cards some comfort. The airline has won several awards from independent organisations. It was the first low cost carrier to provide self service check-in in airports and to ensure that passengers were able to pre-check themselves online.

Organisation 12
This company is a national carrier and the largest airline in Africa in terms of the number of route networks both in Africa and overseas, and flies to more destinations than any other African airline. This airline was established 1 February 1934. The carrier has evolved over the years and most of the business is done online. In fact, the cheapest air tickets are only available online. Organisation 11 was the only carrier in South Africa that was given permission by the South African Civil Aviation Authority to allow its passengers to use cell phones on flights as part of a pilot to determine the feasibility.

Organisation 13
This airline was founded in April 1994 specifically for South Africa and the Southern Africa market generally. It operates as both a passenger and cargo carrier and its route network is growing steadily. Organisation 13 is headquartered in OR Tambo International Airport in Johannesburg. The airline conduct most of its business online – including buying and issuing tickets, checking one's trip and online check-in.

Organisation 14
This privately owned airline was established in 1967 and restyled in 1995. In January 2006, the company changed its name and corporate identity. It created its own niche market by targeting its operations to smaller regional hubs and towns in Southern Africa. The airline is in crucial strategic partnership with other two prominent airlines in South Africa. It flies to more local destinations than any other carrier, operating more than 3000 flights in a month. These flights service more than 25 destinations in Southern Africa. Tickets purchasing, bookings, online check-in, changing reservation and paying can be done online.

Organisation 15
This online shop is a subsidiary of a renowned "traditional" supermarket chain which was established in the 1930's in South Africa. Nowadays, the supermarket chain's footprint has expanded substantially through franchising partnerships, and it now operates in several African countries,

Middle East, and Australia. Groceries sold via the online shop include food, wine, and homeware. The online shop also provides cell phone airtime, clothes, gifts, and financial services (credit card, insurance, and personal loans). ICT is an important enabler and delivery chain of this supermarket. The Holding Company of this supermarket is listed as one of the top 100 listed companies in companies in the Johannesburg Stock Exchange.

Organisation 16

Organisation 16 is an online shop which is a division of a prominent supermarket franchise Group. The Group employs 38 000 people and yields a yearly turnover of around USD6.76 billion. The Group was founded in 1967 as a family business and it was listed in the Johannesburg Stock Exchange the following year. It has now grown into a prominent retail chain. As part of the growth the online shop (Organisation 16) was established. The website of the online shop enables customers to view and buy groceries, general merchandise, school stationary, wine and liquor, gifts and flowers, and entertainment devices. The online shop also offer services such as finance (Go Banking), recipe centre, and catalogues.

Organisation 17

Organisation 17 is one of the most successful online retailers in South Africa, providing books, CDs, DVDs, games, electronic products, etc. The company is owned by South African based and Johannesburg Securities Exchange multinational media companies. The Group that owns Organisation 17 is the biggest media company in the emerging markets and has attained a significant proficiency in e-commerce. Other than selling its own products and services, the website of Organisation 17 also serves as a marketplace for the sellers and buyers. In real essence, this enables the customers of Organisation 17 to sell and buy from each other. The website of this online shop provides guidelines on how customers can place and sell their products in its website. These products are viewed by thousands of fellow Organisation 17 shoppers. When a customer wants to buy a product placed on the website of the online shop by another customer, Organisation 17 processes the order on behalf of the seller and advises the seller to ship the product to the buyer. Once the product has been delivered, Organisation 17 passes the money to the seller.

Organisation 18

This organisation is an airline based in the Middle East, but with operations in South Africa. Its operations in South Africa must, inevitably, comply with the South African legal requirements, including those that deal with information security. The airline has a dedicated South African website. As part of this study, I analysed and studied this website to determine compliance with the legal and policy aspects pertaining to information security. Organisation 18 was started in October 1985. The airline has grown steadily with a fleet of 153 aircraft, 100 destinations, and operates in 66 countries. Over and above allowing online services, this airline is also mobile-enabled. This means that you can use your cell phone to do the following: do your booking; check-in and select or alter your seat on the move; receive your boarding pass on your cell phone; see your itinerary, request a meal and book a chauffeur-driven service; check when your guests arrive or when your flight is due to leave; view for the type of aircraft, its cabin features and in-flight entertainment before you depart.

Organisation 19

This airline is owned by a government of a certain country situated in Southern Africa. Like Organisation 18, this carrier should comply with the relevant South African legislation since it has operations in the OR Tambo International Airport, Johannesburg, South Africa. The airline was established in the 1980's and started making some profit after it went through a corporatisation process. This led to the operations of this national carrier being housed under a parastatal entity. Organisation 19 allows customers to buy tickets and book flights online.

Organisation 20

The company was established in 1977 as a national carrier in one of the East African countries. It was 100% owned by the government until it was privatised in 1996. This made it the first national carrier to be successfully privatised. The airline is considered one of the leading operations in the Sub-Saharan. The company is listed in the Kenyan and Tanzanian Stock Exchanges. It has routes and destinations in Africa, America, Europe, Middle East, and Asia. Similarly to Organisations 18 and 19 in the above paragraphs, this organisation has an obligation to comply with the South Africa laws since it also operates in South Africa. Passengers can procure tickets and book flights online. Other than Credit Cards, payments can also be made via the mobile money facility, MPesa.

Organisation 21
This organisation is a division of one of the leading booksellers in South Africa. The bookselling company was founded in Johannesburg, South Africa. In 1999, the company added another element on its bookselling business by providing a sophisticated lifestyle experience to its customers (book readers) in its bookstores by introducing coffee shops inside. Later on the bookseller introduced an online bookshop. As time progressed, it became more than just an online bookselling entity since there are many other products and services that can be bought in its website. These include music, films, games, vouchers, and electronic devices.

Organisation 22
This company is a South African based independent online retailer which started trading in November 2003. Initially, it operated solely as a bookseller, but later on added music, DVDs, and games in 2005. This online shop sells commercial, professional, and academic books. There are more than a million different titles and thousands of games, CDs, and DVDs in its catalogue. The website of this company has a detailed Credit card security policy; something which I find to be highly commendable.

Organisation 23
Just like Organisations 21 and 22 in the above paragraphs, this entity was initially established to sell books, but has later added other products in its websites. These include games, movies, multimedia, music, stationery, and toys. The company in which this division (Organisation 23) belong to is one of the oldest retail chain which started trading in 1896, making this retail brand to be a century old. This South African based company has operations in the Southern Africa.

Organisation 24
This online retailer is based in South Africa and specialises in selling computing products and services such as computers, accessories, networking, hardware, modding, games, and some services.

Organisation 25
This group of companies is a South African cinema company. Its head office is in Johannesburg. During the course of doing the fieldwork of this study, this company operated cinemas in 22 locations in South Africa. It is the second-largest cinema operator in South Africa. In December 2001, this company launched Africa's first all-digital cinema complex in Johannesburg. Customers are able to book movies and to purchase tickets online.

Organisation 26
This is the largest cinema operating company in South Africa. It is owned by one of the biggest media groups and it operates 54 movie complexes in South Africa. Customers are able to book movies and to purchase tickets online (eTickets).

Organisation 27
This opulently stylish hotel (5 stars) is located in Johannesburg upmarket northern suburbs. Guests are able to make room reservations online.

Organisation 28
This four star hotel is situated in Parktown, Johannesburg. Guests are able to make room reservations online.

Organisation 29
This four star hotel is situated in Rustenburg. The land around this hotel has been game fenced and there are various types of animals. Guests are able to make room reservations online.

Organisation 30
This five star hotel is situated in Rustenburg. It was designed to cater for the camping and training of local and international sports teams. It has advanced conference, sports and medical facilities. Customers are able to make room reservations online.

Organisation 31
This hotel group operates several four and five star hotels, resorts and bush lodges.

Organisation 32
This South African hotel group has 45 years experience and its portfolio has about 90 hotels worldwide.

Organisation 33
This hotel group was established in South Africa in 1985. The group operates hotels in five distinct brands – one to five stars. It operates 54 hotels in southern and eastern Africa.

Organisation 34
This organisation is the biggest distance learning university in Africa and the longest standing dedicated distance higher education provider in the world. Its head office is in Pretoria and it was established in 1873. It enrols approximately one-third of all the South African university students. At the time of doing the fieldwork of this study, this university had more than 300 000 students.

Organisation 35
This university is situated in Johannesburg and it was granted full university status in 1922. It is one of the only universities in Africa that have been ranked by two international rankings as leading higher education institutions in the world.

Organisation 36
This hotel group was established in Johannesburg in 2001. It operates several hotels, lodges and country houses.

Organisation 37
This broadcasting and media group was established in 1994 and its listing in the Johannesburg Stock Exchange was terminated in 2007 after a successful private equity transaction. It operates four popular radio stations and an independent news service.

Orgnaisation 38
This broadcasting and media group has major shareholding in five radio stations and a TV channel in South Africa.

Organisation 39
This online retailer was established in 1999 in Johannesburg. Before the establishment of Kalahari.net in 2009, it was the largest online marketplace in South Africa. The user base of this marketplace are buyers and sellers. During the course of the fieldwork of this study, this company had about 30 000 registered sellers and 380 000 buyers. The number of unique visitors to this online marketplace was more than one million per month.

Organisation 40
This global car renting company is owned by a group of companies. Most of the vehicles in its pool are less than a year old. This company was the first company to link car rental with airline travel in

the America’s Willow Run Airport in December 1946. The company started operating in South Africa in 1967 by opening its head-office in Bloemfontein. By the mid 1980s, the South African operation became the biggest car rental service provider outside of the United States of America. The South African business started to expand to other countries in the Southern Africa region. In 1993 the company received SABS 150 9002 quality management system. In the 1990’s the company enabled its customers to book cars and make payments online.

Organisation 41
This car rental company was established more than 40 years ago. It is the second biggest car rental company in South Africa and offers a fleet of just over 20 000 vehicles at 85 locations in different parts of Southern Africa. This company is listed in the Johannesburg Stock Exchange and operates in 150 countries in Africa, Europe and Australia. It employs more than 40 000 employees and provides online renting and payment web facility for its customers.

Organisation 42
This organisation is one of the small car renting companies in South Africa. It was established in 1986 in Johannesburg and has a fleet of just over 3000 renting vehicles. Outside of South Africa, this car rental operates in some countries in Southern Africa. Ckients are enabled to book and make payments online.

Organisation 43
This is a provider of communication services, mobile telephony, and business solutions. The company is listed in the Johannesburg Stock Exchange under the Industrial – Telecommunications sector as a South African-based multinational mobile telecommunications operator, functioning in several African and Middle Eastern countries. The operator was launched in 1994 in South Africa and it is now operating in 21 countries in Africa and Middle East. It is estimated that by 2012 the combined market share of all its operations will register more than 300 million. In August 2005, this operator entered into a venture with Organisation 2 and launched an online bank.

Organisation 44
Organisation 44 is a public telecoms operator listed in New York and Johannesburg Stock Exchanges. The company is a fixed and wireless telecommunications service provider in South Africa. It is a semi-privatised company and the South African government owns 39% equity. The company has approximately 24,879 employees. For many years this company was the only operator handling international connections to and from South Africa on the South Atlantic 3 (SAT3) and South Africa-Far East (SAFE) backbone lines, which constituted the majority of international bandwidth in South Africa, and fixed-line communications. However, its market dominance was neutralised by the arrival of another fixed line operator which started to provide services in 2008. Organisation 44’s infrastructure consists of local copper loops, microwave, fibre optic loops, and wireless connections. It deploys Asymmetric Digital Subscriber Line (ADSL) over Plain Old Telephone Service (POTS) mainly in the inner-city and suburban areas in cities such as Johannesburg, Cape Town, Pretoria, Port Elizabeth, and Durban. It is on this premise that Organisation 44 is the biggest provider of fixed-line broadband in the Republic.

Organisation 45
This fixed line telecommunications operator was launched in South Africa on 31 August 2006 in Kyalami, Johannesburg. It is the first direct competitor to the incumbent telecoms operator. Various licences were issued to Organisation 45, including the PSTS License; they enable the operator to offer an assortment of telecommunications services, except a fully-fledged mobile telephony. In other words, the company can deploy mobile services moderately. Organisation 44 is in fact the first legitimately converged network providing voice and data on one network. The operator delivers its services through various technologies. Corporate customers are serviced by fibre cable or Worldwide Interoperability for Microwave Access connections while consumers are served by Code Division Multiple Access. It has entered into a partnership with SEACOM to build an undersea cable that will

connect South Africa to India and Europe. Through this relationship, this operator will own the cable landing station and all facilities within the South African territory. The reason for much anticipation for Organisation 44's launch was driven by the desire of consumers to see the decrease in telecommunications prices. For many years, the incumbent's monopoly was seen as a big factor contributing to excessive telecommunications and broadband related costs.

APPENDIX B1

PROTOCOL FOR THE SEMI-STRUCTURED INTERVIEWS: INFORMATION SECURITY PRACTITIONERS WITHIN PARTICIPATING ORGANIZATIONS

- How are information security related policies developed in your company?
- In what extent does the legislation influence your information security policies?
- How were the regulatory aspects, like those contained in the King III Report, incorporated in your information security policies?
- How are the following aspects of information security problems provided for in your policies?
    - Malicious Code
    - Hacking
    - Copyright
    - Privacy
    - Patents
    - Trademark
- To what extent are computer system users familiar with the information security policies?

APPENDIX B2

AN EXAMPLE OF A TRANSCRIPTION OF AN INDIVIDUAL INTERVIEW (TRANSCRIBED FROM VOICE RECORDING): INFORMATION SECURITY PRACTITIONER WITHIN THE PARTICIPATING ORGANISATION

Interviewer: "How is information related policies developed in your company"?

Interviewee: "That's an interesting question, I think the first step is identifying what policies are required and like many organizations, you look at the risks I organization and the statuary requirements of the organization and what we do is , we try to identify what type of policy would be most applicable so we also try and consolidate topics under one type of policy for example electronic communication would include internet usage, email usage, insert messaging usage in one policy document instead of having three separate policy document. So, the high level we try and identify what type of policy we need. We try and see structure and then what we also do is , we try and break it up into different levels of policy because we have what we call the information security road map, information security strategy, which is strategic document on one level and then you'll have something like this (he draws the structure on paper) . It's not necessarily a triangle. You'd have strategy here, like a road map document and a strategic document and here, it would be high level policies, so you would identify say on a principle level inflow policy and in our case you identify acceptable usage policy which apply o all users then on the next level you would have something called Standards, which would be more technically orientated to detailed instructions on how to be specific technologies. So you'd have windows, climax, standard and etc. and then the next level would be procedures which would be detailed instructions on a step by step guide of how to secure documents and then what we also have is something called Guidelines. Guidelines sections which was for an example a booklet that summarizes acceptable usage because what typically happens is that in the high level policies, legal policies has to review them because it has to be tied from a legal point of view. It would be very difficult for the end-user to read it and actually read it because if you want to read it you'll make sense of it.

So that's why we interpret it and put it to user-friendly guidelines document. So this would be guideline, document where you'd be having guidelines where you'll be choosing strong passwords. So coming back to your question , we first take a view of what type of documents we want and then we just break it up into manageable chunks and what we do is for an example policies, what we do is create a working group, so these people will essentially have preventatives from the business, someone from the HR department, someone from the legal department if possible, someone from the IT department and then we had someone from the customer care side, so there was approximately about five to six people and we also used an external consultant just to provide input in terms of what the industry chains are, just to put right guidance around that and we workshop the policy and once we were reasonably happy with the content, then what we did was we took it up to the higher level co-operate body information

Steering committee. We sent the policy to them with reading all these documents. Essentially what we did is, we took the policy documents and distilled them into bullet points and into a presentation and highlighted contextual point to them, for example it might be something around no unauthorized software allowed on workstations so the debate comes as to what is unauthorized software. There are a lot of people who want to download software so that they can test on a net word point of view like your engineers and so on. So all the contentious point and the sirloin point are highlighted presented to the steer-come and if they are happy with them we get the chairman of the steer-come to sign off the policies.

Interviewer: “Who is the chairman of the steer-come in terms of position”?

Interviewee: “So, at that stage when we sign off the policy was chaired by the CIO of the organization but it has subsequently changed**”.**

Interviewer: “In what extend does the legislation influence your information security policies”?

Interviewee: “I am not a 100% sure but what we do is we rely a lot on legal and regulation department to review the document and make sure that there’s no violation of the current legislation and so when we develop policies ourselves, we don’t consciously look at the legislation and try and mend that scientifically against for an example, the promotional access information act or any of those type of act. Information security and then mend that to the policy, we relied on the legal department to do that and I think to some extend they did review that and made sure that it was compliant to legislation.

Interviewer: “How were the regulatory aspects like those contained in the King II Report incorporated in your information security policies”?

Interviewee: “For an example in the King II that influenced heavily the composition of the information security steering committee and as I said before that is the body that formally approves policies, it did but just taking King II into account, we didn’t directly observe, it was more around the government structure that we looked at”.

Interviewer: “How are the following aspects off information security problems provided for in your policies”?

- Malicious Code
- Hacking
- Copyright
- Privacy
- Patents
- Trademark

Interviewee: “For Malicious Code, what we do is we split that in two sections policy section and standard section. Policy section was more of a high level policy section around Malicious Code for example the principle section would be that there need to be mechanisms to ensure that Malicious Code is check on for workstations on very frequent basis. That would be on a principle statement that would be in a policy. In the standard we’d have specific guidelines around checking for Malicious Code, so there must be anti-virus installed, there must be anti-spyware installed. When you open a file, it must check for Malicious Code before. The uploading system needs to cater for that and also the anti-virus software, so essentially it will split into two sections just a policy and then a Malicious Code standard because its around how anti-virus technology must be set up, how anti-sperm technology must be set up and so on, so that’s how we address that how we address that in our policies”.

Interviewer: “So, which server addresses Malicious Code”?

Interviewee: “We have a policy called Protection against Malicious Code policy and standard”.

Interviewer: “How do your policies make provision regarding hacking”?

Interviewee: “From a hacking perspective, we address this up to the users and the organization. There was a number of statements around general users and ownership and around the fact that users acknowledge that the system that they are using belong to the organization and the software that they are using belong to an organization and therefore they have obligation on their side to make sure that they don't interfere in their systems and do not try and sub verb to mechanisms or any controls, so that's on one hand and we also made it very explicit in the usage policy that because the assets belong to the organization, the organization has a right to monitor and intersect any communication via end-users, if they feel that there is a bridge of security promises. So that was actually specified in the usage policy".

Interviewer: "And copyright"?

Interviewee: "Copyright, we also mentioned that in the accepted usage policy that there shouldn't be any type of illegal software, downloads or installations and so on. That was by the explicit in the policy, the copyright and regarding all staff in the accepted usage policies, what we did is we provided guidelines and submitted it to the end-users so that they can read it, and then we also created a movie where it demonstrated good and bad behavior around copying of software, installing unauthorized software".

Interviewer: "And, privacy"?

Interviewee: "Privacy, we didn't specifically address that. The only time we did refer to privacy is when we did what I mentioned before, that the organization has a right to do monitoring, if it feels that it has been misused, so we didn't go into a detailed privacy statement".

Interviewer: "The technical guys, did you have some policies that say to them, 'we respect user's privacy'? For example you know that technicals for example can read some emails".

Interviewee: "What we did have is there was a number of system administrators and they had privileged access to user-id, a generic account that was used by systems to log into each other, they also knew the password into that, so the risk is that they could have logged in with a generic application account and viewed someone's confidential information and the only things that would come up on the log, would be an exchange account, so that we did with the system administrators is we got a document that that regarded them in to sign about acceptance of the usage policy but we wanted them to physically sign it to say that they acknowledge that they have been given privileged access to user information and there was a number of clauses in there, it was a one or two page where we say that they will safe guard the policy, report if there's specific incident or suspected bridge and that they will not use any of the privileged information themselves. We got all the end-users to sign it and we kept that file and it was more than deterrent than anything else so they know that they have signed a document to say that they are conscious of the fact that they will not abuse it".

Interviewer: "Patents"

Interviewee: "Patents, we didn't address directly in our policies, same with trademark. What was the interesting about that is that we found that some organizations in different countries were trying to use the company brand to scam people, so they would send an email to someone with a brand and say 'congratulations you've won such amount of money, trying to be an organization so that they could scam them. The same with, a job interview where they were offering jobs for people and they had to pay a registration fee so they are pretending to be a company and run-off with the money".

Interviewer: "But, technically people can go onto a website and cut and paste and so on, there isn't much that the organization can do".

Interviewee: "Yes, also because it's cross border, that becomes very complicated, so other organizations investigate these issues, try and shut down these fake websites and so on".

Interviewer: “Talking about the cross border because your organization is multinational, the policies that you have in South Africa, are they applicable in other countries”?

Interviewee: “I think in theory yes, they are because we made sure that we had someone in HR that does not represent South Africa but was representing the HR. We have the HR department for South Africa and accrued HR department looking after all twenty countries based in South Africa, with a clue that they will be translated all the other organizations and so it was those policies written with those organizations in mind”.

Interviewer: “To what extent are computer system users familiar with the information security policies in South African companies”?

Interviewee: “I think generally that’s always the problem because people always feel that information security policies get in the way and it’s something that hinders them from their work, and generally it’s very difficult to get people to pay attention to policies and all that. In our organization it depends on which topics of the policy, I think there’s high degree of awareness around for an example, choosing strong passwords, so for example, you know how to use a strong password because of some of the awareness campaigns but also because we have mechanisms that actually forces them to do that, so when they log into that domain, they have to have these eight characters, it cant contain letters of their first names, it has to have at least a numeric, lower case and upper case, so its forcing them to do that. In other areas something that’s not as well-known for example fishing scams, the familiarity around that is less, same with other things around internet usage, email usage and so on, people are reasonably aware and familiar with information security.

APPENDIX B3

PROTOCOL FOR SEMI-STRUCTURED INTERVIEW: INFORMATION SECURITY OR CYBER LAW EXPERT

- At what extent does the legislation in South Africa influence the composition of the business continuity and disaster recovery related policies at company level?
- To what extent are the regulatory aspects like those contained in the King III Report incorporated in companies' business continuity and disaster recovery policies?
- How are the aspects of business continuity and disaster recovery provided for in legislation and companies' policies?
- To what extent are employees in companies familiar with the information business continuity and disaster recovery policies?

APPENDIX B4

AN EXAMPLE OF A TRANSCRIPTION OF AN INDIVIDUAL INTERVIEW (TRANSCRIBED FROM VOICE RECORDING): INFORMATION SECURITY OR CYBER LAW EXPERT

Interviewer: "At what extent does the legislation in South Africa influence the composition of the information security related policies at company level"?

Interviewee: "It's not the only legislation that influences but it's also things like KING II code and those people want to limit the exposure to legal risk. They will try and mitigate it in terms of what employers do with information within the organization and the best way to achieve that is through company policies. So, typical policies would be things that relate to electronic communications, email and internet usage, that would say' you need to keep company information confidential and cant disclose trade secrets' and so they try to limit the legal risks through that. Specific legislation that impacts policies, electronic communications and transactions act, according to that legislation, the way that communications is defined includes SMS, voice, it includes transactions that are done through websites and what companies actually do, they use those definitions in their company policies so that the legal risks on that edge in accordance with the terms that are used by the legislation".

Interviewer: "Would you say companies are cautious about the legal requirements or their policy will be mobile"?

Interviewee: "One of the observations that I have is that people buy batches of policies and they do ISO compliance for instance 27001 and they will immediately implement those policies rather than drafting the policies based on the legislation and lead of requirements, they would just use those policies. The awareness is that they should have a policy but they don't have the awareness to actually make the policy relevant to them, they'd rather purchase just broad generated policies and apply those, although they have a policy it's not implemented".

Interviewer: "Regarding the KING II, to what extent does that also influence the information security policies"?

Interviewee: "Well, in the KING II code it speaks about an awareness of the implications of technology on a business and the KING II code says that an organization that implements the KING II code must also be aware of risks that emanate from technology and they must also put in place measures to reduce those risks and based on that, people who are implementing the KING II code look at information security practices because of the technology risks that I mentioned earlier".

Interviewer: "Let's take this one by one; does the legislation address viruses"?

Interviewer: Hacking?

Interviewee: "The Electronic Communications and Transactions Act has provisions that relate to Cyber Crime and it speaks about unauthorized, access and interceptions and so while its not using the word hacking or something like that, it is actually referring to that, and the main thing that comes out is that if anybody deals with information in an unauthorized way, it can be criminalized and will result in a criminal offence".

Interviewer: "And copyright"?

Interviewee: “There’s the copyright legislation in South Africa and the copyright legislation however is not updated in terms of the new digital environment so its quiet outdated and doesn’t speak directly to information security. It speaks about computer programmes but doesn’t deal directly with how people access information online and what they can do with it and how they can prevent those risks”.

Interviewer: “And privacy issues”?

Interviewee: “There’s a bill that’s about to come into forces, its called the Protection of Private Information Bill and that deal with personal information of consumers and all organizations can do with that information and it lists principles on how to do their information, it says how to keep it secure, you must not disclose it to anyone whose not authorized, it has specific principles but unfortunately that legislation is not yet enforced”.

Interviewer: “In terms of patents and trademarks that relates to IT do you think they are addressed by the legislation?

Interviewee: “So the Patent’s Act has a real problem in terms of software programmes in that it says that it’s not in the software programmes and business methods that you can patent, but the problem is that they are actually being patented by software programmers. So there’s a loop in the system and companies are taking advantage of it because the state doesn’t exactly examine something if it is patentable. It may not deal directly with the information security but it clears someway with technology. The problem with this loophole is that it may discourage investors and innovation. How would a software investor or programmer invest on something that may not be patent anyway? It means the software source code can be used by one’s competitors. Trademarks, it speaks about what you can do with a logo and what cant do, and the way that it is, is quite broad, so it can actually deal with the using a logo online in an unauthorized way in the way the act is structured, it does kind of deal with that although it doesn’t say’ specifically online’. Its broadly interpreted saying you may use a logo in an unauthorized way so it does deal with it indirectly”.

Interviewer: “But do you think with information security, the manager is for example concerned with trademark or some other department’s problem”?

Interviewee: “I think within the departments they often shift the blame, so the legal would say that it’s on IT problem if it relates from a website and then if it’s a trademark issue IT would say that it’s a legal problem and they generally shift blame for these things. So think that within the organization what they must do is that when they are saying that this policy is going to be implemented, they must actually say who is going to implemented it, which department is responsible for it, because at the moment, I do think that they do shift blame on departments and organizations is not well defined, who should be managing information security and sometimes what happens is that they just have an IT department and they will got to legal and say ‘now you will also do information security’, but there isn’t somebody specifically designated to do.

Interviewer: “What’s your view regarding contradictory provisions in the law; for example, privacy versus access to information”?

Interviewee: “The trends has been that the new legislation introduces some terms that are in conflict with the other legislation, so I think that what needs to happen is that when people are drafting a new legislation like the protection of personal information bill, they must also look at other legislation that impacts that and make sure that the terminology match because very often you find that they are speaking about same thing but they are calling it different things and so, otherwise developing to have two terms for the same thing or it’s a bit in conflict with each other or its more than the new legislation is in conflict with the old legislation from the terminology perspective or that it hasn’t been thought through. So, in the implementation of it one legislation says that you cannot do this, and the other legislation says that you can”.

APPENDIX C

AN EXAMPLE OF A DOCUMENT OBTAINED FROM AN ORGANISATION

BUYS INC. ATTORNEYS
E-MAIL LEGAL NOTICE

1. This email legal notice is enforceable and binding on the recipient / addressee in terms of sections 11(1) to 11(3) of the Electronic Communications and Transactions (“ECT”) Act 25 of 2002.

2. This e-mail transmission contains confidential information, which is the property of Buys Inc. Attorneys (“Buys Inc.”). No person, other than the recipient (so indicated by the sender) may use or disclose the contents of this message, links or attachments hereto, to any person whatsoever. Unauthorised disclosure and/or use may result in civil and criminal liability.

3. The information in this e-mail, links or attachments thereto is intended for the attention of the addressee only – if you are not the intended addressee/recipient, you are hereby notified that any disclosure, copying or distribution of the contents of this e-mail transmission or the taking of any action in reliance thereon or pursuant thereto, is strictly prohibited. Should you have received this e-mail in error, please delete and destroy it immediately and notify the sender.

4. The e-mail address of the sender may not be used, copied, sold, disclosed, shared or incorporated into any database or mailing list for spamming and/or other online marketing practices without the prior consent of the sender and/or Buys Inc.

5. Under no circumstances shall Buys Inc. Or sender of this e-mail be liable to any party for any direct, indirect, special or consequential damages, including, without limitation, any loss of profits, business interruption, loss of programs or other data on information handling systems or otherwise, even if Buys Inc. or sender of this e-mail have been expressly advised of the possibility of such damages.

6. Any agreements concluded with Buys Inc. by using electronic correspondence shall only come into effect once Buys Inc. indicated such contract formation in a follow up or return communication and always subject to the requirements of the ECT Act and contract law in general.

7. No email correspondence sent to Buys Inc. shall be deemed to have been received until Buys Inc. has responded thereto. An auto-reply shall not constitute such “response” for purpose of this clause. Return e-mail messages blocked by Buys Inc.’s virus detection and/or filtering applications shall not be deemed to have been received by Buys Inc. and/or the addressee.

8. No warranties are made or implied that any employee and/or contractor of Buys Inc. is or was authorised to create and send this communication.

9. Buys Inc. reserves the right to intercept, filter, view, block, delete, access, copy, read and act upon this e-mail message and all e-mail messages send as reply messages to this e-mail message or the address of the sender.

10. Buys Inc. retains the copyright in all e-mail messages and attachments sent from its communications systems insofar as such content is original and subject to copyright. The recipient / addressee is hereby licensed to open and read the messages and/or attachments only – all other rights are reserved unless so indicated by the sender and/or Buys Inc.

11. The views and opinions expressed in this e-mail message do not necessarily reflect the views and/or opinions of Buys Inc. if this e-mail message is used for purposes unrelated to the official business of Buys Inc., Buys Inc. shall not be liable for any damage, liability, infringement or loss caused by the contents of this message and the sender shall take full responsibility therefore in his/her sole and personal capacity.

12. Subject to urgent and interim relief, all disputes and/or disagreements and/or liabilities, in any manner related to the:
    - 12.1. Interpretation, validity, access to and enforceability of this e-mail legal notice;
    - 12.2. Content (including message headers, links and/or attachments) of this e-mail;
    - 12.3. The time and place this email was sent and/or delivered; and/or
    - 12.4. The identity of the sender,

    shall be referred to urgent and confidential arbitration in terms of the expedited arbitration rules of the Arbitration Foundation of Southern Africa and such arbitration shall be conducted in Cape Town in English.

13. The law of South Africa shall govern this e-mail message and legal notice.

14. Information disclosures required by law:
    - 14.1. Full name: Buys Inc. Attorneys;
    - 14.2. Registration number: 2001/013344/21
    - 14.3. Vat Registration number: 4280197882
    - 14.4. Directors: Reinhardt Buys, SA
    - 14.5. Postal address: P O Box 12215, Mill Street, Gardens, 8010;
    - 14.6. Street address: 24 Dunkley Square, Gardens, 8010;
    - 14.7. Web site: http://www.buys.co.za;
    - 14.8. Blog: http://blog.buys.co.za/; and
    - 14.9. Forum: http://forum.buys.co.za/

15. This e-mail legal notice shall at all times take precedence over any other e-mail disclaimer(s) attached to return e-mails addressed to any person with an Buys Inc. e-mail account.

16. Please contact the following person should you have any questions regarding this e-mail legal notice: reinhardt@buys.co.za.

APPENDIX D

AN EXAMPLE OF THE EMPLOYEE INTERCEPTION CONSENT

RATIONALE

[COMPANY NAME] of [COMPANY STREET ADDRESS] has a legal obligation and duty to:

- Identify, manage and mitigate the risks and dangers associated with the use of electronic communication facilities by employees;
- Practice good corporate governance;
- Ensure the safety and security of its technology network; and
- Provide a safe and healthy working environment.

[COMPANY NAME] employees have a constitutional right to privacy, dignity and free speech that extends, although subject to certain limitations, to the workplace.

The proper manner through which [COMPANY NAME] can balance its abovementioned duties and obligations with the constitutional rights of employees is by way of:

- [COMPANY NAME] monitoring employee's electronic communications if so required; and
- Employees providing the necessary undertakings and consent detailed herein.

UNDERTAKING AND CONSENT

1. I, the undersigned Employee records, acknowledges and agrees that:

1.1 during the course of my appointment by [COMPANY NAME] (Pty) Ltd reg. no. 1998/022574/07 ("[COMPANY NAME]"), I shall become acquainted with, gain personal and indepth knowledge of and have direct access and use to:

1.1.1 strategic, sensitive and confidential information of [COMPANY NAME];

1.1.2 [COMPANY NAME]'s Equipment; and

1.1.3 [COMPANY NAME]'s Communication Facilities;

1.2 the security of the Equipment, Communication Facilities and the protection of confidential information are of crucial importance to the business of [COMPANY NAME], who has a legitimate proprietary and commercial interest therein which it is entitled to protect;

1.3 should the security of the Equipment or Communication Facilities be breached and/or confidential information be disclosed, it may cause [COMPANY NAME] considerable financial loss and legal liability;

1.4 [COMPANY NAME] may also be liable for the actions of persons who use [COMPANY NAME]'s Equipment or Communication Facilities for unauthorised or illegal purposes; and

1.5 the only effective and reasonable manner in which [COMPANY NAME]'s legitimate proprietary and commercial interests may be protected so as to avoid financial loss or liability, is by way of the furnishing of the written undertakings detailed below by myself.

2. In return for the right to access and use [COMPANY NAME]'s Equipment and Communication Facilities and in the interest of the protection and maintenance of [COMPANY NAME]'s security and nondisclosure responsibilities, I agree and acknowledge that [COMPANY NAME] has the right to:

2.1 Intercept any Communications;

2.2 Intercept any Records; and

2.3 Intercept any information directly associated with Communication.

3. The rights detailed above shall only apply to Communications initiated, received or conducted through or on the Equipment or Communication Facilities of [COMPANY NAME] and will only be relied upon when reasonably required with due regard to the constitutional freedoms and privacy of those concerned;

4. I agree and acknowledge that I read and understood the provisions of the new [COMPANY NAME] Electronic Communications Policy, available at [PLEASE INCLUDE WEB SITE ADDRESS WHERE THE POLICY WILL BE PUBLISHED]; and

5. For purposes of this undertaking, the following words shall have the following meanings:

5.1 "Intercept" includes filter, scan, block, redirect, access, disrupt, copy, print, disclose, retain, use, collect, delete and/or record, in any format and in any manner;

5.2 "Equipment" means computers, desktops, servers, routers, laptops, telephones, cell phones, electronic handheld devices, facsimile machines, pagers, software, hardware and/or similar Equipment owned by, licensed to or rented by [COMPANY NAME];

5.3 "Communication Facilities" include Internet access, email access, instant messaging, sms and/or use of any Equipment for purposes of:

5.3.1 initiating, receiving or storing of Communications; or

5.3.2 accessing, creating, copying, distributing, sharing and deleting Records.

5.4 "Communications" mean and include:

5.4.1 oral and verbal utterances of an employee in or during a formal meeting where the business of [COMPANY NAME] or related matters are discussed;

5.4.2 the transfer of any information whether speech, data, text, images in any format through Communication Facilities; and

5.4.3 access to or use of the services available on the Internet, including email, web sites, file transfer, video conferencing, voice over IP, chat rooms and bulletin boards; and

5.5 "Records" means any content, document, record, file, data, information, picture, download, graphic, depiction, representation or software that is created, used, accessed, disclosed, copied, stored, received or delivered by an employee, regardless of the format thereof.

[name of employee]

APPENDIX E

AN EXAMPLE OF OWN WORK DECLARATION

I ____________________________ (Student number: __________________) am a student registered for _______________________ in the year ___________. I hereby declare the following:

- I am aware that plagiarism (the use of someone else's work without their permission and/or without acknowledging the original source) is wrong.
- I confirm that the work submitted for assessment for the above course is my own unaided work except where I have explicitly indicated otherwise.
- I have followed the required conventions in referencing the thoughts and ideas of others.
- I understand that the University of the Witwatersrand may take disciplinary action against me if there is a belief that this in not my own unaided work or that I have failed to acknowledge the source of the ideas or words in my writing.

Signature: __________________________ Date: _________________________

APPENDIX F

Papers published

APPENDIX F1:

Dagada, R., Eloff M.M., Venter, L.M. (2009) *Too many laws but very little progress! Is South African highly acclaimed information security legislation redundant?* Proceedings of the ISSA 2009 Conference, Editors: Hein Venter, Marijke Coetzee and Les Labuschagne, pp 327 - 346, ISBN 978-1-86854-740-1, 6 – 8 July 2009, Johannesburg, South Africa, available online at http://icsa.cs.up.ac.za/issa/proceedings.htm

TOO MANY LAWS BUT VERY LITTLE PROGRESS! IS SOUTH AFRICAN HIGHLY ACCLAIMED INFORMATION SECURITY LEGISLATION REDUNDANT?

[1]R Dagada, [2]MM Eloff, [3]LM Venter
[1]University of the Witwatersrand, [2]University of South Africa, [3]SAP /Meraka UTD and University of South Africa

[1]Rabelani.Dagada@wits.ac.za
[2]eloffmm@unisa.ac.za
[3]Lucas.venter@sap.com

ABSTRACT

South Africa has myriad laws that address information security related issues. One such law is the Electronic Communications and Transactions Act of 2002 (ECTA), which is highly regarded internationally. A study, which forms the basis of this paper, found that not all provisions of this legislation that deal with information security are implemented by both the government and information security practitioners in corporate South Africa. The study found that the South African government has a relaxed approach to implementing some of the legal provisions regarding information security. The ECT Act agitates for the appointment of cyber inspectors who have powers to inspect, search and seize. A magistrate or a judge may issue a warrant requested by the cyber inspector. Although the legislation had good intentions, the government has not yet appointed the cyber inspectors. Although the ECT Act was in part intended to curb the spam emails, the effect of the Act is practically very little. The study also found that some of the information security laws are ambiguous, for example, the Patent Act. Some of the laws pertaining to information security are very old; they were in effect introduced before the Internet was used for commercial purposes. These include the Merchandise Marks Act of 1941 and Copyright Act of 1978.

The findings of this study reflect that information security practitioners were not really familiar with the avalanche of information security related legislation. Be that as it may, the contents of the IT policies from some of the organisations that participated in this study contain the provisions of legislation were catered for in the policies. This should be attributed to the fact that although information security practitioners were not consciously trying to comply with legislation, they relied heavily on the international standards. Most of these standards are in line with the requirements of the South African information security related legislation. In other words, corporate information security policies are within the framework of the Constitution of the Republic and the applicable legislation by default. They are not consistent with constitutional and legislative provisions by conscious effort on the part of the information security practitioners. It is in this premise that this study contains a concept model for legal compliance for information security at the corporate environment. This model embodies the contribution of the study.

KEYWORDS

Information Security, Legislative Compliance, Information Security Policies, Model for Legal Compliance

1. INTRODUCTION

Most organisations around the world as well as in South Africa have developed web sites for information and business related purposes. Some of these Websites merely display information about the organisation, whilst others offer some interactivity with customers. The Internet revolution is developing rapidly due to electronic commerce (e-commerce) (Mattord, 2007; Plotkin & Fagan, 2003). It is on this premise that most organisations are striving to catch up. De Kare-Silver (2001) and (Irwin, Yu, & Winsborough, 2008) noted that it is a daunting task for organisations to master the new environment. He puts it this way: "There is a new game in town and it is now about learning and embracing the new factors for success." However, 'the new game in town' has brought with it a number of challenges. According to Chorafas (2001), the challenges brought by the Internet to the corporate environment include information security risks, threats and crime. The bottom line is that rapid development of technology has an impact on business systems. Negative forces of technology on businesses should be managed.

Negative challenges brought on by technology do not affect corporate actors only. Other constituencies of business, particularly clients, are affected by the growth and diffusion of technology in business. Increasingly, clients have to conduct transactions on the Internet, receive advice from Websites, and interact with business online. The new culture, e-market, raises questions of security and trust. Chorafas (2001) claims that security is e-commerce's Achilles heel. Dugan, Egan, Kraus & Hancock (2003) report that the business-to-consumer component of e-commerce may be affected by reservations regarding security breaches. On the other hand, the credit card is the most common online payment option and thus both e-commerce customers and merchants are vulnerable to potentially high levels of fraud due to stolen cards and illegally acquired card numbers (Boynton, 2007; Chorafas, 2001:250). Although new technical measures are being established to deal with online fraud, these techniques are not necessarily infallible; a perfect method of encrypting has not yet been developed (Bond, 2002:189). It is on this premise that information security measures cannot be left to technical methods only (Bond, 2002:188).

The remainder of the paper is structured as follows – literature review, the research problem, the research methodology, findings of the study, concept model of legal compliance for information security at the corporate environment, and conclusion. For the purpose of this paper, the words Information and Communications Technologies (ICT), and Information Technology (IT) will be used synonymously.

2. LITERATURE REVIEW: A BRIEF OVERVIEW

The literature review a brief overview of the issues that are related to e-commerce, information security threats, risks and crime, and legal and policy aspects of information security. It also provides a brief legal framework of cyberlaw in the South African context.

2.1 Information security risks, threats and crime

The introduction mentioned the importance of using information resources. Whilst information resources are essential in participating in e-commerce and the information economy, they are not exempt from risks, threats and crime (Vorster & Labuschagne, 2005; Targowski, 2003). It is therefore advisable for any organisation that uses information resources to have the necessary information security (Gupta, Chandrashekhar, Sabnis & Bastry, 2007; Collin, 1997). Information security provides e-commerce merchants and consumers with the safety and the sense of freedom from risks, threats and crime. Feiler (2000) observes that in e-commerce four different places are involved, that is - the location of the user, the location of the Web server, the location of the Web owner and the virtual location of the site, and thus information security is an essential concern. Privacy is one of the challenges regarding information security (Tondel, Jaatun & Meland, 2008; Lobree, 2001). This, according to Chorafas (2001), is a major problem to any financial transaction in the e-commerce environment.

The processing of e-commerce transactions raises the issue of information security. Windham (1999) reports that during the early era of e-commerce, the Internet was generally regarded to be an unprotected medium. This perception, rightfully so, continues to persist. News of hackers and online fraudsters made headlines and led to fear amongst millions of potential electronic shoppers. They thought the Internet was not a secure environment to provide confidential information. This, according to Windham (1999), held the information economy back from even earlier advancement. Viruses and other forms of hostile code (malware) are universally experienced as an information security problem. The infection rate continues to grow and this affects the e-commerce participants negatively (Champlain, 1998; Tirado, 2008). Heiser (2001) reports that malware has the ability to penetrate firewalls, hijack Virtual Private Networks and also defeat digital signatures. Aggressive code is the most well known source of security lapse. Heiser (2001) lists several examples of malware. These include worms, Trojan horses and macro viruses. In view of these concerns information security is crucial in the business environment. Below is a discussion on policy aspects to be considered for information security.

2.2 Policy aspects to consider when providing information security

It was mentioned in the previous section that some organisations post their information security policies on their Websites. This demonstrates corporate diligence in explaining their commitment to online business security. It was also stated that these policies deal with issues such as the usage of credit cards and other personal data. Windham (1999) provides an example of how America Online posts a privacy policy on its Website regarding the kind of information it collects about people who visit its Website. America Online also explains what it does or does not do with the collected personal data. Tudor (2001) reports that information security policy is formulated to inform all individuals who operate within an organisation regarding how they should conduct themselves when it comes to ICT information security issues. In some instances policies are formulated because of regulatory requirements (Turner, 2000; Irwin, Yu & Winsborough, 2008). Developing information security policies just for the sake of satisfying regulatory obligation is not good enough (Myers & Riela, 2008; Tudor, 2001). Information security policy is used as a communication tool amongst the information system stakeholders (Champlain, 1998). Turner (2000:191) declared that the advancement of the information economy in terms of the e-commerce rapid growth puts an obligation on government and organisations to develop information security policies and regulatory solutions. During this era of the information economy, information security policies will assist in providing users with security and privacy certainty (Champlain, 1998; Bhilare, Ramani & Tanwani, 2009). Turner (2001) notes that the differences in policy approaches amongst key role players and countries make it difficult to provide a better information security policy and regulatory framework. Although this difficulty takes place at macro level, it manifests itself at micro (organisational) level. Whilst these can be regarded as generic policy aspects, below is a South African legal framework on e-commerce and information security.

2.3 Legal framework of e-commerce and information security in South Africa

There has been rapid use of e-commerce in South Africa; hence the need to develop legislation that would provide security to Internet consumers and merchants (Dunlop, 2005). *South African common law* was not sufficiently addressing issues related to the security of electronic transactions (Goodburn & Ngoye, 2004). According to Dunlop (2005), the South African government did not confine its concern just to information security, but intended to provide a legal framework that would address security, transparency and infrastructural commercial development (Hofman et al. 1999). The e-commerce initiatives that are based on a sound legal framework would enable South Africa to become a leading technology power in the African continent (Dunlop, 2005). It is on this basis that the *South African Department of Communications* established an ICT investment cluster in May 1998 to create a legislative framework on issues relating to e-commerce and information security (Groenewald, 2000). For focus purposes, the following is the research problem.

3. THE RESEARCH PROBLEM

Legal and policy aspects are important in the provision of information security. Although several authors have written about legal and policy aspects regarding information security in the South African context, none of them has explained how these aspects are used in the provision of information security in the South African corporate environment. The question arises as to whether the *Constitution of the Republic* (1996), the *Electronic Communications and Transactions Act* of 2002 (2002), the *King 2 Report* (2002) and other information security related legislation at macro level and the organisations' policies are used by South African organisations in their endeavours to protect their information resources.

Both the 2002 and 2004 website compliance surveys in South Africa "painted a bleak picture of non-compliance and general indifference towards laws and regulations governing websites and the online sale of goods and services in South Africa" (Buys Incorporated Attorneys, 2004). In 2002 26% of South African website operators claimed that they were not aware of the compliance requirements. It is astonishing to note that this number increased in 2004 by 5% to 31% (Buys Incorporated Attorneys, 2004).

The failure to comply with the law, according to Buys Incorporated Attorneys (2004), has led to an increase in website crime: "During March 2002, a defamatory statement posted to the website of *Kick-Off* magazine, ended in the High Court. A month later the *Department of Health* investigated an illegal online pharmacy in Table View and in June of the same year, the *Gauteng Metro Police* attempted to close down a website that warned motorists of speed traps around Johannesburg." The problem is exacerbated by the fact that most South African companies do not comply with the requirements of Chapter 7 and Part III of Chapter 3 of the ECT Act. They do not seem to realise that failure to comply with the provisions of the law exposes their websites to huge risk and liability. Of the 1 550 websites surveyed by Buys Incorporated Attorneys (2004), the Telkom website (www.telkom.co.za) was the only one to score a full 100% compliance rate.

Other than the aforesaid website compliance survey conducted by the Buys Incorporated Attorneys in 2002 and 2004, it appears there had never been any substantial study that focuses on the compliance of information security related legislation by organisations in South Africa. Moreover, it remains to be established whether the existing company policies are in line with the national and international legal regime. The lack of results with regard to consideration of legal and policy aspects in the South African corporate environment seems to indicate the need for research in this field. There is a gap in the literature as to how information security legal policy and legislation add value to the corporate environment within the South African corporate context. The literature does not show if South African organisations are complying with the national legal and policy framework regarding information security.

Within this context, following questions are posed:

- How are South African companies employing legal and policy prescriptions to enhance information security?
- To what extent do the South African legislation impacts on the endeavours to curb information security related problems? and

- To what extent are organisations in the South African integrating information security legal requirements into their policy formulation and implementation?
-

3.1 Sampling and profile of the organisations

Twenty-two organisations participated in this study. These organisations are from different industrial sectors. These include IT, telecommunications, mining, services, academia and research, regulatory authorities, public administration, construction, insurance, and banking sectors. It is important to mention that the banking sector dominated all other industrial sectors. This is because the four biggest banks in South Africa – namely Standard bank, First National Bank, Amalgamated Banks of South Africa, participated in this study. In addition to the aforesaid organisations, three organisations (IT governance consultancy and two law firms) were involved. Purpose sampling was employed since the participating organisations were purposefully selected due to the contribution they would add to the study.

3.2 Data collection and analysis

This study used the generic techniques for qualitative data collection and analysis. This study satisfied the principle if triangulation by employing multiple data-gathering methods and sources. Data gathering methods include individual interviews, key informant interviews, observation, and policy documents analysis. Interview protocols for both the individual and key informant interviews were semi-structured. Interviews were analysed by using open coding. A frequent comparative method was applied to analyse data within and between interviews. Content analysis was applied to analyse the content of interviews. The process involved the instantaneous coding of raw data and the construction of categories. Data collected through document analysis was analysed by comparing it with the South African legal framework pertaining to information security.

4. FINDINGS OF THE STUDY

This section addresses findings that were obtained through interviews, documents analysis, and observation.

4.1 Findings obtained through interview

4.1.1 The Board of Directors are not involved in the formulation of information security policies

This study found that the involvement of the Board of Directors in the establishment of the information security policies is very minimal or non-existence. This is in conflict with the spirit of good cooperate governance as espoused by the King II and Draft King Reports. This was confirmed by a Senior Lecturer at a South African university, an expert in information security law: "*King III will have more IT governance provisions. IT governance and security will become the responsibility of the Board of Directors. According to the Draft King III, IT security is an important element of the overall business efficiency and sustainability.*" This study found that policies in all 22 organisations that participated in this study are actually approved at the Chief Information Officer's (CIO) level. The CIO would convene an ICT Steering Committee which is constituted by representatives from various departments. The problem is that most of these representatives are actually not really senior. This shows that most organisations do not take information security seriously. However in the Draft King III Report, information security policies should be approved by the Board and that the IT Steering Committee should be chaired by the Chief Executive Officer (CEO) and "*all Group Executives are expected to serve in the IT Steering Committee.*" Therefore, flouting this provision demonstrates deviance from compliance requirement.

4.1.2 Very few organisations in South Africa incorporates legislation requirements in the information security policies

Legislation in South Africa has a lot of impact in policy formulation. A certain information security legal expert had observed that: "*The problem is that very few IT security experts and practitioners are* *conscious about this. Technology people are more familiar with the standards; unfortunately there is myriad of legislation and governance internationally and in South Africa*." In South Africa, one of the crucial pieces of legislation is the Electronic Communications and Transactions Act of 2002. This Act deals with the removal of legal barriers to electronic transactions and provides security framework for both the merchants and buyers. The legal expert continued: "*You would expect most information security practitioners to be familiar with sections that deal with security related aspects in this Act, but unfortunately very few security experts and practitioners incorporate the Act's security requirements in the IT policies. I really think this is highly irregular because it exposes consumers who use websites of the companies that are not integrating the requirements of the Act for e-commerce purposes.*" A Johannesburg-based Managing Director of the IT legal firm concurred: "*One of the observations that I have made is that people buy batches of the policies and they do ISO compliance, for instance '2700' and they will immediately implement those policies rather than drafting the policies based on legislation*." Most IT departments are aware that they should have information security policies but they do not have the awareness to actually make the policies relevant to them, "*they'd rather purchase just broad generated policies and apply those.*" This means that corporate security executives are not diligent in the execution of security mandate. In addition, they are lax, lack commitment and are characterised by unprofessional demeanour. This account of security professionals and approach to their vocation permeated overwhelmingly during the data collection stage.

During an interview with the Information Security Officer of an agency which provides IT services to the whole provincial government, she indicated that legal department or outside lawyers were not involved in four of their information security related policies and there was no effort to ensure that these policies integrate the legislation requirements. However, she emphasised that the drafting of their Records Management Policy and Data Retention Schedule is guided by the legal requirements. An Information Security Manager in one of the biggest mobile telecommunications network in South Africa and the African continent, confirmed that when the IT department drafts the security policies they "*don't consciously look at the legislation and try and mend that scientifically against, for example, the Promotion of Access to Information Act*." However, interestingly they "*relied on the legal department to do that and I think to some extent they did review that and made sure that it was compliant to legislation*."

4.1.3 Legal provisions to fight cyber crime are redundant

Some of the South African information legal information security provisions were highly acclaimed when they were introduced, but unfortunately they are not yet implemented. These include provisions to prevent viruses, hacking, and industrial espionage. Provisions to fight against the aforesaid IT related crimes are contained in Chapter 8 of the ECT Act of 2002. Hacking, industrial espionage, viruses, spam emails and other cyber related crimes are characterised by an unauthorised access to, interception of or interference with data and thus they are supposed to be tackled by cyber inspectors. A Senior Lecturer who specialises in information security law said the provision for the cyber cops is: "*Articulated in Chapter 12 of the Electronic Communications and Transactions Act*." It is unfortunate that this provision has not yet been implemented even though the Act was passed more seven years ago.

After realising that cell phones were contributing to the commission of criminal activities, law makers in South Africa established the 'Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002'. Amongst other things, this Act stipulates that the buyers of the pre-paid SIM cards should be registered by cell phones network operators so that the law enforcement agencies could identify them if and when their cell numbers are used to plan or to commit crime. A legal expert indicated that: "*the Department of Justice will announce a date in which the registration of the people who buy SIM cards commences. The delay in implementing this requirement is not justifiable, especially when you consider the fact that the Act was passed in 2002.*"

Chapter 10 of the ECT Act agitates for the establishment of the Cryptography Providers. This is one the legal measures to prevent IT related crimes. Cryptography concerns itself with the hiding of information. In an email communication the message would get encrypted and impossible to read by an intruder. The whole message will be gibberish. "*To date the Director General of Communications has not yet established a register of Cryptography Providers*."

4.1.4 Legal provision that deal with unsolicited communication has serious loophole

Unsolicited emails, famously known as spam emails, are addressed in Chapter 7 of the Electronic Communications and Transactions Act of 2002. This Chapter of the aforesaid Act deals with consumer protection. The spam emails are dealt with in Clause 45 which prohibits unsolicited commercial communications to the consumers. However, during the interviews, interviewees indicated that this prohibition is not effective. Sellers of the goods, products and services are using a loophole in the Act to send chains of unsolicited messages to the consumers: "*The Act says the sender should give the recipient an option to cancel the subscription. However, consumers are ignorant and thus they are flooded with spam emails. In real essence, the first email that is sent is unsolicited, but it is legal because it gives the recipient an option to opt out. Usually, recipients don't opt out and thus the subsequent emails cannot be defined as unsolicited because the consumer is deemed to have opted to receive the adverts since he did not opt out. This is entirely within the law*." The problem is that most banking clients in South have received unsolicited emails which were attached with viruses and spyware.

4.2 FINDINGS OBTAINED THROUGH DOCUMENT COLLECTION AND ANALYSIS

Information security related policies were collected from 16 of the 22 organisations that participated in this study. The collected policies were analysed against information security related legislation. It is important to state that only half of the 16 companies whose policies were analysed have integrated information security legal provisions into their policies. Two of the eight companies that have integrated legislation in their policies had only incorporated legislation requirements in their Records Retention Schedules; the rest of their information security policies do not make any reference to any law. Paragraphs below provide results of the document analysis.

4.2.1 Policies regarding hacking

Hacking has much to do with access control. This is addressed in our Information Security Policy, and Interception & Surveillance Policy. The relevant legislations are the Promotion of Access to Information Act; Electronic Communications and Transactions Act; and the Interception Act.

4.2.2 Policies regarding intellectual property, copyright, and trademarks

Intellectual Property is gradually becoming an important asset amongst the South African companies. According to the information contained in the few collected policies, it includes assets such as, but not limited to – 'websites content, website source code, software developed within a particular company, software developed by employees, product packaging, trademarks, domain names, marketing information, and the like'. Copyright is addressed by the Intellectual Property Policy. The objective of this policy is to formulate a framework for the establishment, protection, registration, maintenance, management and use of ICT Intellectual Property. This policy is applicable to all employees, third parties, external contractors, and ICT Intellectual Property related contracts entered into by employees acting on behalf of the organization. The relevant legislation is the Intellectual Property Law Amendment Act of 1997, Copyright Act of 1978, Merchandise Marks Act of 1941. The problem is that some of the aforementioned laws are very old and were introduced before the Internet was used for commercial purposes. Other relevant policies for the intellectual property, copyright and trademarks are the Information Security Policy and the Data Privacy Policy. It is a matter of extreme concern to note that the majority of the organizations that participated in this study do not have policies that address the protection of intellectual property, copyright and trademarks.

4.2.3 Policies regarding patents rights

None of the companies that participated in this study had a separate policy on patents. Actually, only three organizations addressed the patents protection as part of the intellectual property policy. The researcher concluded that this could be due to the fact that most companies that participated in this study perceive the South African patent law to be ineffective. According to the Patents Act of 1978, computer programmes cannot be patented; however, companies are patenting these programmes anyway. In other words, Companies and Intellectual Property Registration Office (CIPRO), an organ of the state responsible for patents registration – does not respect the Act responsible for patents.

4.3 Findings obtained through observation

The researcher investigated the websites of the 22 organizations that participated in this study. The purpose of the observation was to determine if the websites complied with the following information security legal requirements: availability of legal notice, terms and conditions available as hyperlinks, liability disclaimers available as hyperlinks, compliance with the provisions of Chapter 3, Part II and Chapter 7 of the Electronic Communications and Transactions Act, positioning and implementing legal notice correctly, availability of legal notice that is printable or saveable as required by section 11(3) of Electronic Communications and Transactions Act, and availability of policies that address websites legal compliance. Table 1 below reflects the findings of the observation.

Table 1: Number of organizations that are compliant with the legislation governing websites and e-commerce.

ASPECT OBSERVED	NUMBER
Websites with legal notices at all	17
Websites with terms and conditions available as hyperlinks	7
Websites with liability disclaimers available as hyperlinks	11
Websites with legal notices that address the provisions of Chapter 3, Part II and Chapter 7 of the ECT Act	5
Websites that position and implement legal notices correctly	2
Website legal notices that are printable or saveable as required by section 11(3) of the ECT Act	2
Organizations that have policies that address websites legal compliance	5

From Table 1 above, one deduces that most companies in South Africa are not complying with the legal requirements of the websites. This may expose the consumers to cyber crime during electronic transactions. It appears most IT and information security practitioners are not familiar with the requirements of the Electronic Communications and Transactions Act of 2002 regarding consumer protection. Although 17 out 21 websites that were observed have legal notices, their legal notices are very elementary in nature. These legal notices, and/or 'terms and conditions' do not make provisions regarding some of the following legal requirements – 'definitions and interpretation, allowed usage and license, intellectual property rights and domain name use, software and equipment, disclosures required by section 43 of the Electronic Communications and Transactions Act, changes and amendments, privacy, hyperlinks to third parties, security, disclaimer and limitation of liability, removal and correction of content, interception of communications, entire agreement and severability, agreement in terms of Section 21 of the Electronic Communications and Transactions Act, applicable and governing law, and legal costs'. Irrefutably, table 1 conclusively show limited, partial compliance. In some websites there is not attempt to comply with relevant policies at all.

5. CONCEPT MODEL OF LEGAL COMPLIANCE FOR INFORMATION SECURITY AT THE CORPORATE ENVIRONMENT

This section suggests a model whereby legal requirements are incorporated into the information security endeavours – policy formulation, implementation, and monitoring. This model is an intellectual property of the writers and can be seen as a synthesis of theory, practice and cognitive perspectives gained over the years of practical experience. The model was necessitated by the main finding of this study which reveals that both the government and corporate South Africa were not implementing some of the information security legal provisions. This model may be very useful to policy formulators, directors of the boards, ICT executives, and information security practitioners. A graphic representation of the model reflected in Figure 1

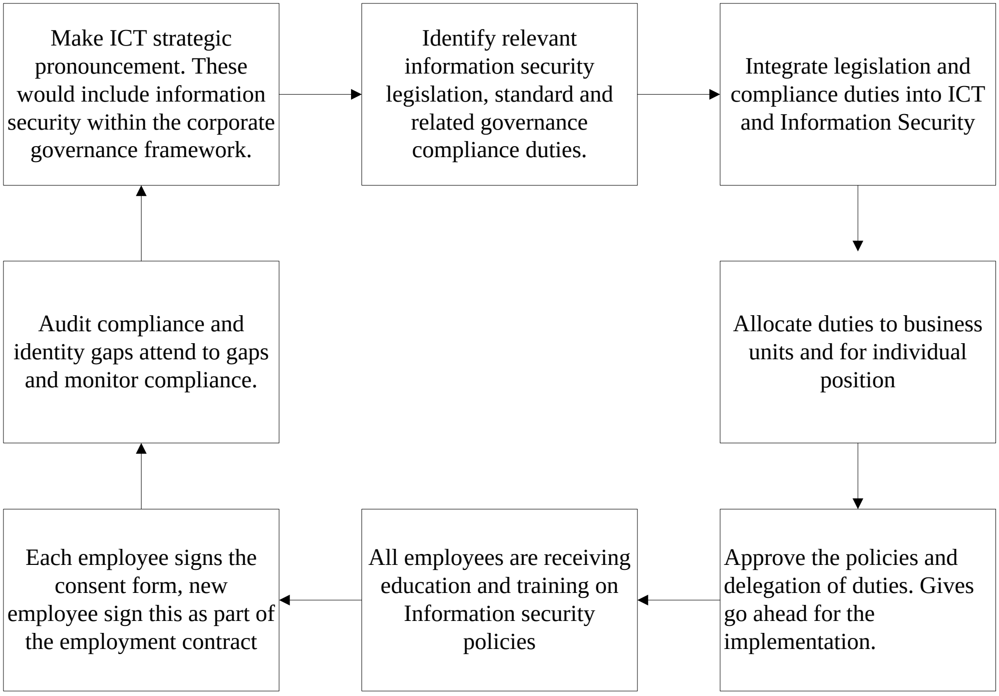

Make ICT strategic pronouncement. These would include information security within the corporate governance framework.
Identify relevant information security legislation, standard and related governance compliance duties.
Integrate legislation and compliance duties into ICT and Information Security
Allocate duties to business units and for individual position
Approve the policies and delegation of duties. Gives go ahead for the implementation.
All employees are receiving education and training on Information security policies
Each employee signs the consent form, new employee sign this as part of the employment contract
Audit compliance and identity gaps attend to gaps and monitor compliance.

Figure 1: A concept of legal compliance for Information security policies formulation, implementation and multitasking.

According to the Draft King III Report, IT strategic planning, risk management and information security is the primary responsibilities of the Board of Directors. One does not expect the Board to be involved in a detailed process regarding the formulation of the information security policies, but they should rather make broader pronouncements within the business strategic direction and sustainability, corporate governance, standards, and legislation framework. The Draft King III advices that there should be an ICT Steering Committee at the enterprise's executive level. This ICT Steering Committee will include all executives in the organisations and chaired by the CEO. It is the researchers' contention that relevant information security and related compliance duties should be identified at this level. Once this has been done, the next step will be the ICT Department.

The ICT Department is headed by the CIO. According the Draft King III Report, the CIO must be business oriented and must be an interface between IT and business. S/he would obviously serve in the ICT Steering Committee and thus s/he take the identified information security legal provisions and related compliance duties and translate them into information security policies. The drafted information security policies will then be taken by the CIO to the ICT Steering Committee for consideration and comment. The Steering Committee will allocate duties business units and/or individual positions. The policies will then be taken to the Board's Sub-Committee for Risk Management for approval. All employees will then be trained regarding the information security policies. They will also be asked to sign the acceptance forms. The Board's Sub-Committee on Risk Management will audit compliance and identify gaps. Thus, the overall intention of the model is to prioritise information security, elevate the profit of business security, and ultimately address corporate security lapses.

6. CONCLUSION

There are more than ten laws that deal with information security in South Africa. The title of this paper poses a very thought proving question – are these laws effective enough in addressing information security challenges in corporate environment? The answer is no. Information security provisions that are contained in certain laws are not yet implemented. There is also a deliberate disregard of the information security legal provisions by some companies and the government entities. It was reported in this paper that most IT and information security practitioners were not familiar with the information security legal requirements. It is perhaps in this premise that most South African companies do not comply with the requirements of the law regarding information security related matters.

In some instances the attitude of the South African government towards its own laws has been lukewarm. The Electronic Communications and Transactions Act, 2002, agitate for the appointment of cyber inspectors who have powers to inspect, search and seize. A magistrate or a judge may issue a warrant requested by the cyber inspector. Although the legislator had good intentions, the government has not yet appointed the cyber inspectors. This paper reported the confusion related to the legality of the of the software patents in this country. This matter should be brought to the attention of the legislators. Some of the laws pertaining to information security are very old; they were in effect introduced before the Internet was used for commercial purposes. These include the Merchandise Marks Act of 1941; Copyright Act of 1978; and the Patents Act of 1978. Having said all these, one would conclude that although information security and the legislation thereof do not reflect a perfect marriage; their marriage, with its imperfections, remains necessary.

7. REFERENCES

Bagby, JW 2003: E-commerce law: issues for business. Ohio: Thomson.

Bhilare, DS, Ramani, AK, & Tanwani, 2009: Information security assurance for academic institutions using role based security metric: an incremental approach. Proceedings of the International Conference on Advances in Computing, Communication and Control, pp 535-540, 23-24 January 2009. New York: ACM.

Bond, R 2002: New economy equity: navigating security and legal issues in digital business. Worcester: John Wiley & Sons.

Boynton, BC 2007: Identification of process improvement methodologies with application in information security. Proceedings of the 4th annual conference on information security curriculum development. New York: ACM.

Buys, R 2004: 2004 South African website compliance survey results nothing to be proud of. Buys Inc. Attorneys/Legalsentry.

Champlain, J 1998: Auditing information systems: a comprehensive reference guide. New York: John Wiley & Sons.

Chorafas, DN 2001: The Internet supply chain: impact on accounting and logistics. New York: Palgrave.

Collin, S 1997: doing business on the Internet. London: Kogan page

Conkling, WR & Hamilton, JA 2008: The importance of information security spending: an economic approach. Proceedings of the 2008 spring simulation multiconference, pp 293-300. San Diego: The Society for Computer Simulation, International.

De Kare-Silver, M 2001: E-shock: the new rules – Internet strategies for retailers and manufacturers. New York: Amacom.

Draft Report on Governance for South Africa, 2009. The Institute of Directors in Southern Africa and the King Committee in Corporate Governance. Johannesburg.

Dugan, JC, Egan, EM, Kraus, AD & Hancock, EM 2003: Privacy & e-commerce in the United States. (In: Plotkin, ME, Wells, B & Wimmer, K eds. 2003: E-commerce law & business (Volume 1). New York: Aspen Publishers).

Feiler, J 2000: Managing the web-based enterprise. London: Morgan Kaufman.

Godburn, D & Ngoye, M 2004: privacy and the Internet (In: Buys R & Cronje, F eds. 2004: Cyberlaw: the law of the Internet in South Africa. Van Schaik Publishers, pp 97-112).

Heiser, J 2001: An introduction to hostile code and its control (In: Tipton, HF & Krause, M eds. 2001: Information security management handbook. London Auerbach Publications, pp 475-495).

Hofman, J, Johnston, D, Handa, S & Morgan, C 1999: Cyberlaw: a guide for South Africans doing business online. Cape Town: Ampersand.

Irwin, K, Yu, T, & Winsborough, WH, 2008: Avoiding information leakage in security-policy-aware planning. Proceedings of the 7th ACM workshop on privacy in the electronic society, pp 85-94. New York: ACM.

King Report on Corporate Governance for South Africa 2002. The Institute of Directors in Southern Africa and the King Committee in Corporate Governance. Johannesburg.

Lobree, BA, 2001: E-mail security (In: Tipton, HF & Krause, M eds. 2001: Information security management handbook. London Auerbach Publications, pp 55-82).

Martin, J 1996: Cybercorp: the new business revolution. New York: Amacom.

Mattord, HJ, 2007: Rethinking risk-based information security. Proceedings of the 4th annual conference on information security curriculum development, 28-29 September 2007. New York: ACM.

Merriam, SB 1998: Qualitative & case study applications in education. San Francisco: Jossey-Bass Publishers.

Myers, JP, & Riela, S, 2008: Taming the diversity of information assurance & security. Journal of Computing Sciences in Colleges, 23(4), pp 173-179. Consortium for Computing Sciences in Colleges, USA.

South Africa, 1941: Merchandise Marks Act. Pretoria: Department of Trade and Industry

South Africa, 1978: Copyright Act 98. Pretoria: Department of Trade and Industry.

South Africa, 1978: Patents Act No. 57. Pretoria: Department of Trade and Industry.

South Africa, 1993: Trade Marks Act 194. Pretoria: Department of Trade and Industry.

South Africa, 1997: Intellectual property laws amendment Act. Pretoria: Department of Trade and Industry.

South Africa, 2000: Promotion of Access to Information Act. Pretoria: Department of Justice and Constitutional development.

South Africa, 2002: Electronic Communications and Transactions Act. Pretoria: Department of Communications.

Targowski, AS 2003: Electronic enterprise: strategy and architecture. Hershey: IRM.

Tirado, I 2008: Business oriented information security requirements development. Proceedings of the 5th annual conference on information security curriculum development, pp 56-58. New York: ACM.

Tondel, IA, Jaatun, MG, & Meland, PH 2008: Security requirements for the rest of us: a survey. IEEE Software, pp 20-27. Los Alasmitos: IEEE Computer Society Press.

Tudor, JK 2001: Information security architecture: an integrated approach to security in the organization. Boca Raton: Auerbach.

Turner, C 2000: The information e-conomy: business strategies for competing in the global age. London: Kogan Page.

Vorster, A, & Labuschagne, L 2005: A framework for comparing different information security risk analysis methodologies. Proceedings of the 2005 annual conference of the South African Institute of Computer Scientists and Information Technologists on IT research in developing countries, pp 95-103. SAICSIT.

Windham, L 1999: Dead ahead: the web dilemma and the new rules of business. New York: Allworth Press.

APPENDIX F2:

Dagada R, and Eloff M.M., (2013), Integration of policy aspects into information security issues in South African organisations, *African Journal of Business Management*, Vol. 7(31), pp. 3069-3077.

INTEGRATION OF POLICY ASPECTS INTO INFORMATION SECURITY ISSUES IN SOUTH AFRICAN ORGANISATIONS

Rabelani Dagada
Wits Business School
University of the Witwatersrand
South Africa

M.M. Eloff
Institute for Corporate Citizenship
College of Economic and Management Sciences, University of South Africa

Abstract

Information for individual organisations should always be secured. Organisations need to protect their information from attackers or competitors as these could lead to law suits or loss of business. With the more advanced network technology, information security risks and threats are believed to be on the increase and becoming even more sophisticated. This paper assesses how South African organisations integrate legal and policy aspects when they deal with information security issues. Qualitative research methods were employed to gather and analyse data for the study. Results show that participation by top management in the provision of information security policies is very minimal in organisations. Again, most information security practitioners are not familiar with the legal and policy aspects that they are supposed to integrate in the implementation of information security and thus most organisations in the country are not complying with the law.

KEY WORDS

Security risks, South African, organisations, information security polices, legal compliance

Introduction

In South Africa, as in many other countries, many organisations have developed websites for information and business related purposes (Beatty, Reat, Dick, & Miller, 2011; Bond, 2002). While some of the organisations have their websites merely display information about the organisation, others have gone further to offer interactivity with clients. However, research shows that there are challenges, brought by the Internet to the corporate environment, which are exacerbated by information security risks, threats and crime (Fumey-Nassah 2007; Sha, 2008, Johnston and Warkentin 2010).

Organisations need to protect their information from attackers or competitors as these could lead to law suits or loss of business. In other words, information for the organisation should always be secure. Information Security refers to “measures adopted to prevent the unauthorized use, misuse, modification, or denial of use of knowledge, facts data or capabilities” (Maiwald 2004:4). Put differently, it is the preventative measures put in place to guard information and capabilities hence keeping these safe from threats and any exploitation (ibid). While it may be argued that there are several kinds of information security issues; and that different security problems may lead to different legal issues, and may need different management intervention and policies, it is not the aim of this paper to focus on a specific information security issue. This paper tries to understand what South African organizations are doing regarding integration of information security legal requirements into their policy formulation and implementation

South African organizations and their clients are not immune to cybercrime (Bruns & Huth, 2011; Dunlop, 2005). The South African government therefore passed the Electronic Communications and Transactions Act, No. 25 of 2002. The Institute of Directors in Southern Africa (King II Report) (2002) also deals with information security issues. Prior to the proclamation of the Electronic Communications and Transactions Act, No. 25 of 2002 and the King II Report, South African e-commerce merchants and customers relied on common law (Dunlop, 2005). The legislation that was introduced has given e-commerce participants confidence in transacting over the Internet (Venter, 2005; Tran, 2010). However, there are no studies undertaken yet to assess how South African organisations integrate legal and policy aspects when they deal with information security issues. This study, therefore, aims at investigating such aspects. Thus the study attempts to answer the question:

> To what extent are organisations in South Africa integrating information security legal requirements into their policy formulation and implementation?

To answer the question, the study employed a qualitative research approach. One-on-one interviews, websites analysis, and document analysis were techniques used to gather data. Results of the study show that the participation of the Board of Directors in the provision of information security policies is very minimal. Again, most information security practitioners are not familiar with the legal and policy aspects that they are supposed to integrate in the implementation of information security and thus most organisations in the country are not complying with the law. It is therefore recommended that governance aspects of ICTs should be taken seriously by the Board of Directors and other responsible structures and should be given priority due to their technical nature. Nonetheless, there should be an interrogation to the alignment of the ICT strategy to the overall business strategy and the impact of ICT in the sustainability of the organization.

Significance of the study

This study may provide important insights into the future application of legal and policy aspects in the provision of information security in the South African corporate environment. Companies, Boards of Directors, ICT executives, information security practitioners, e-commerce participants, and policy formulators may use the findings of this study as a resource and guide. It is envisaged that the findings and recommendations of this study may be transferable and applicable to other contexts and countries. The study will contribute both theoretically and practically in achieving compliance with legislation when implementing information security.The originality of the contribution of this study to the academic and industry knowledge-base has benefited from an additional contextualised corporate description that can enhance the understanding of the intricacies of making use of legislation to improve information security in South African organisations.

Problems with Information Security

Threats on Information Security, have increased dramatically in the past few years; especially with the more advanced network technology the threats are believed to be on the increase and becoming even more sophisticated (Mlangeni & Biermann, 2005; Johnston and Warkentin 2010). In line with this argument, is Kyobe (2005: 2) who argues that computational models are overly complex and therefore require an enormous amount of historical data, but, unfortunately, this is not always available in some organisations. He further argued that “while information confidentiality, integrity and availability have been emphasized in most models, the evolving nature of threats and technology makes use of these three critical aspects of information security, alone, inadequate” (ibid). Other researchers are also of the opinion that “a sufficiently big set of historic cases must be available for significant probability calculations” (Canal 2005:3).

Maiwald (2004:11) notes that new technologies have simply evolved much faster than security measures put in place; hence it is difficult if not impossible to assure that something is secured. He therefore suggests that, as the industry continues to search for the final answers, individuals and organizations have to define security as best as they can. This means organizations need to exercise due care and due diligence in the management of their information systems. According to Harris (2003) "Due care are steps that are taken to show that a company has taken responsibility for the activities that take place within the corporation and has taken the necessary steps to help protect the company, its resources, and employees. Due diligence refers to the continual activities that make sure the protection mechanisms are continually maintained and operational". This means responsible parties should ensure that due care actions that can be verified or measured are put in place. Due diligence requires ongoing actions whereby individuals or organizations actually have hands on things to guard and maintain preventative processes (Harris, 2003; Chai, Kim & Rao, 2010).

Measures to deal with information security threats

The protective measures against password cracking are similar to those used for traditional password cracking. Skoudis (2004) and Doinea (2009) advised that weak passwords should be eradicated from the system. Nowadays it should be made more difficult for the hacker to guess the password than it was years ago when there were no distributed passwords (Logan & Clarkson, 2005; Summer, 2009). The information security management should establish a policy that compels users to create passwords that are longer than a minimum length (Micco & Rossman, 2002; Bala, 2008). The aforementioned statement proves that technical defence measures should be based on a policy framework rather than just employment of protective technologies. According to Skoudis (2004; Savola, 2007), the information security staff should occasionally run a password-cracking tool against their users' passwords to distinguish the weak ones before the hacker does. Should the weak passwords be found, there should be an approved procedure to rectify this. Users should be educated regarding the selection of better passwords.

To deal with the *distributed denial-of-serv*ice attacks, the information security personnel should ensure that critical network connections have enough bandwidth and redundancy to prevent easy attacks (Manion and Goodrum, 2000). Skoudis (2004) and Katz (2006) reported that lower connection speeds can easily be overwhelmed by the attacker. The *distributed denial-of-service* attacks cannot just be eliminated by having sufficient bandwidth; additional techniques for dealing with these attacks should be employed (Nolan & Levesque, 2005:33). This includes the installation of intrusion detection systems to foresee a possible attack (Sukhai, 2004 and Kesh, 2007). Skoudis (2004:136) described the intrusion detection systems as network burglar alarms – "listening to the network for traffic that matches common attack signatures stored in the [intrusion detection system's] database.

Skoudis (2004) and, Fenz and Ekelhart (2009) claimed that the best protective measure against distributed port scanning is to close down all redundant services in your network. Most relay attacks take place outside an organisation's own network and thus there is little you can do to stop such attacks. It is therefore necessary to ensure that systems are protected by applying security patches and closing down all unrelated services (Stoecklin-Serino, 2009). The aforementioned assertions once more proves that technical measures are not the panacea for ICT security problems. It is therefore necessary to work together with law enforcement officers in dealing with the relay attacks. Equally, data that is transmitted across the network should be encrypted to prevent active sniffing attacks (Summers and Bosworth, 2004; Braz, Fernandez and VanHilst, 2008). The best way of dealing with these kinds of attacks is to empower users to employ certain tools, both from a technical and an awareness perspective. Again, this proves that technology measures cannot be useful in the absence of policy and legal protective defence mechanisms (Zhang, Deng, Li, Wu, Sun, & Deng, 2011; Deane, Ragsdale, Rakes, & Rees, 2009).

Policies and awareness

The ICT ethically related risks, threats and crimes are difficult to counter. This should be attributed to the fact that usually the technical security controls are not effective as protection mechanisms (Schneider, 2000:32; Lamprecht, 2004). Ethical problems such as social engineering, for example, are attacks targeting the human element (Berti and Rogers, 2004:152; Chang, Wang & Shen, 2010). It is on this basis that protective measures need to focus on administrative security defenses (Johnston and Warkentin 2010). These measures are constituted by policies, users' awareness and education. Schneider (2000:30) agitated that policies should be introduced and publicised to the whole enterprise as a measure to counter ethically related problems. Policies are very useful in providing guidelines on how people should behave.

The research approach

This study employed a qualitative approach whereby one-on-one semi-structured interviews, websites analysis and document analysis were techniques used to collect data The reason for using the qualitative approach is that respondents could constitute a rich and valuable source of information (Kalof, Dan & Dietz, 2008; Devers & Frankel, 2000). Again, qualitative data collection techniques such as interviews help in exploring the meanings of situations, and uncertainties which may not be accessible in quantitative techniques.

Participants and sampling

Forty-five South African organisations were both purposively and conveniently included in the study (Cresswell, 2007; Merriam, 1998). The sampling was purposive in that participants were chosen based on the contribution that they could make to the study. That is, those which seem to be data-rich cases for an in-depth study were selected as participants (Blaxte, Hughes & Tight, 2010; Bless & Higson-Smith, 1995). The sampling was convenient in that only those situate in South Africa were targeted to reduce travel and other communication expenses as the researchers were based in the country. Organisations involved in the study came from different industrial sectors such as banking, transport, online retail, hotel, broadcasting, and telecommunications. These included the energy, mining, insurance, banking, telecommunication and services industrial sectors. In addition to information security practitioners and executives in the South African corporate environment, the study also involved cyber law and information security experts.

Data collection techniques

This study used generic techniques for qualitative data collection and analysis (Walliman, 2001; Blaxter et al. 2010). The study satisfied the principle of triangulation by employing multiple data-gathering methods and sources (Maswera, Edwards, & Dawson, 2009; Walsham, 2006). Data-gathering methods included semi-structured interviews, websites analysis, and documents analysis.
The interview was a particularly suitable data collection method for the environment concerned, and made it possible to gather useful information concerning the types of research questions (Hanford, 2009; Dey, 1993; Dargie, 1998). Interviews provided the opportunity for direct contact with the participants in the study, and the ability to obtain facts directly from the research participants. Websites analysis was used as a data collection method to determine websites' legal compliance. This was achieved by analysing the websites of all organisations that participated in this study.

Some data in this study was collected through document analysis (Rowlands, 2005). The study regarding the legal and policy aspects in the provision of information security cannot be investigated without doing document analysis. The reason is that both legal and policy documents should be analysed. The analysis revealed the causal link between them and how they impacted the provision of information security in the South African corporate environment.

Data analysis

Data gained from interviews was analysed using open coding (Cresswell, 2007). A frequent comparative method was applied to analyse data within and between interviews (Merriam, 1998; Henning, Van Rensburg & Smit, 2004). The process involved going through the interview data while marking important sections and adding code to it. While continuing with the process of analysing the data by breaking down into distinct ideas and/or events, any important information in the process was labeled. The names of the labels were decided by the researcher in the study based on his knowledge of the topic as well as considering what was in the content (data). After coding the interview data, the researcher did analysis of the coded data to determine similarities and group them into categories according to their common properties

In a nutshell, content analysis was applied to analyse the content of interview data. The process involved the instantaneous coding of raw data and the construction of categories (Kalof et al. 2008; Merriam, 1998). Data was analysed with the intention to distinguish common patterns and to put together categories; these was weighed against the literature and legislation (Leedy & Ormorod, 2005; Bell, 2006). Data collected through document analysis was analysed by comparing it with the South African legal framework pertaining to information security. Content analysis was also used to analyse the legislation and policy documents from the South African companies which participated in this study.

Trustworthiness

The trustworthiness of this study was guaranteed by fulfilling the needs of triangulation by using various data-gathering methods and sources (Kalof et al. 2008). Moreover, trustworthiness was ensured by using both internal and external validities (Bell, 2006). Internal validity was applied by comparing the research findings with actuality of information security in the South African corporate environment (Merriam, 1998). External validity was accomplished by providing adequately complete descriptions of the context of the study for the reader to compare with other situations (Merriam, 1998; Leedy & Ormorod, 2005).

Ethical considerations

Ethical considerations were observed in this study although some readers may not view this work as sensitive research. Research participants, both at organisational and individual levels, were asked to take part in this study. The requests were conveyed though e-mail letters. Virtually all research participants who accepted to be involved this study approved in writing. Nonetheless, interviewees were at liberty to pull out from the study at any time, with no compulsion to give any explanation. We undertook all measures to ensure that organisations and individuals participating in the study were not caused any harm by doing so; hence we made a commitment to assign a pseudonym to all participants to safeguard their identity and to ensure that any information revealed, either personal or professional, would be treated as completely confidential.

Findings and discussions

Data analysis yielded three main themes, namely: the attitude of corporate South Africa towards information security legislation; the manner in which organisations in South Africa integrate legal aspects in their information security policies; and users' knowledge regarding information security policies.

The attitude of corporate South Africa towards information security legislation

This study found the attitude towards the legal aspects of information security in the South African corporate environment to be negative. The Board of Directors in most of the companies that participated in this study did not provide leadership in the formulation of information security policies. Most organisations in South do not incorporate the requirements of legislation in their information security policies.

The Board of Directors is not involved in the formulation of information security policies

This study found that the involvement of the Board of Directors in the establishment of the information security policies is very minimal or non-existent. This is in conflict with the spirit of good corporate governance as espoused by the King III Report. This was confirmed by a Senior Lecturer who is an expert in information security law in a Law School of one of the prominent South African universities:

> "King III has more IT governance provisions. IT governance and security are the responsibility of the Board of Directors. According to the King III Report, IT security is an important element of the overall business efficiency and sustainability."

Analysis of the data collected shows that policies in the organisations are actually approved at the Chief Information Officer's (CIO) level. The CIO would convene an ICT Steering Committee which is constituted by representatives from various departments. The problem is that most of these representatives are actually not really senior. This shows that most organisations do not take information security seriously. However in the King III Report, it is noted that information security policies should be approved by the Board and that the IT Steering Committee should be chaired by the Chief Executive Officer (CEO) and "*all Group Executives are expected to serve in the IT Steering Committee."* Therefore, flouting this provision demonstrates deviance from compliance requirement.

Very few organisations in South Africa incorporate legislation requirements in their information security policies

Legislation in South Africa has a lot of impact on policy formulation. According to his observations, one information security legal expert narrated the following:

> The problem is that very few IT security experts and practitioners are conscious about this. Technology people are more familiar with the standards; unfortunately there is myriad of legislation and governance internationally and in South Africa.

In South Africa, one of the crucial pieces of legislation is the Electronic Communications and Transactions Act of 2002. This Act deals with the removal of legal barriers to electronic transactions and provides a security framework for both the merchants and buyers. A Johannesburg-based Managing Director of an IT legal firm concurred:

> One of the observations that I have made is that people buy batches of the policies and they do ISO compliance, for instance '2700' and they will immediately implement those policies rather than drafting the policies based on legislation.

Most IT departments are aware that they should have information security policies but they do not have the awareness to actually make the policies relevant to them, "*they'd rather purchase just broad generic policies and apply those.*" This means that corporate security executives are not diligent in the execution of their security mandate. In addition, they are lax, lack commitment and are characterised by unprofessional demeanour. This account of security professionals and their approach to their vocation permeated overwhelmingly during the data collection stage.

Government slowness in implementing information security laws impacts the corporate environment's attitude towards legislation

Analysis also shows that the attitude of corporate South Africa towards the implementation of information security laws is partly affected by the manner in which government performs its responsibilities towards the implementation and improvement of the legislation. Certain provisions in the Electronic Communications and Transactions Act, 2002 have not yet been implemented despite the fact that the legislation was promulgated approximately nine years ago. Nevertheless, South African banks have dedicated teams of information security professionals who 'combat' Internet related crimes. After noticing clients' concerns regarding Internet and Cellphone Banking crime, banks have responded to crime forcefully and with a lot of superiority; to prevent financial losses and reputational damage. a Managing Executive of Digital Banking Channels said:

> We ensure that we have got monitoring systems, behaviour pattern analysis, and early warning systems For example, if a spoofing site is picked up worldwide on the Internet or a phishing email goes out, we typically shut the site down within 45 minutes to two hours. It doesn't matter where it sits in the world.

Banks are also available 24 hours a day to help their customers in case they suspect their Internet Banking accounts are being defrauded. They ensure that transactions via Internet Banking are taking place in an encrypted environment. It is not possible for criminals to intercept encrypted transactions. We also noted that banks were more compliant with the information security aspects of the legislation than all other industrial sectors that participated in this study. A researcher attached to a security institute argued that the South African banks had no choice but to comply with the legal aspects of information security:

> They are however motivated by business considerations rather than solely being loyal to what the legislation prescribes. Companies in other industrial sectors don't have huge volumes of transactions on the Internet like the banking sector has. Consequently, they have very little interest in establishing organs like SABRIC (South African banking Risk Information Centre) or establishing their own sophisticated teams to fight Internet related crimes.

The Head of Enterprise Information Architecture, whose company is the hotel industry, concurred:

> We work with the government through the Business Against Crime initiative, but the government should take leadership when it comes to information security crimes, otherwise companies in South African will end up operating paramilitary entities and that is not good in a constitutional state; I mean we are not in the business of securing the country; we are hoteliers. You can argue that the government is actually breaking the law by delaying the implementation of certain aspects of the Electronic Communications and Transactions Act.

The registration of cellphone SIM cards as required by law was done after seven years of the promulgation of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002'. Criminals in the Internet sphere are getting very sophisticated and the government should ensure that the legislation is updated and implemented in line with the changing times. Therefore, it may be argued that failure by the government to appear to be taking its laws seriously has negative ramifications on the attitude of corporate South Africa towards information security legislation.

The manner in which South African organisations integrate legal aspects in their information security policies

From the analysis, this theme reflects that the delegation of trademark responsibilities is not well defined; legal provisions that deal with unsolicited communication have serious loopholes.

The delegation of the trademark responsibilities is not well defined

Even in organisations wherein the protection of trademarks have been incorporated in policies; the responsibility of implementing them are not defined and this has the potential of rendering the policy redundant. In a certain car hire company, the IT Department has initiated the establishment of the Intellectual Property Policy which, amongst other things, caters for the trademarks:

> Although we have this kind of policy, it is important to stress that we don't regard things like websites and trademarks to be part of the IT Department's domain; they actually belong to the Corporate Communications and Marketing Department. The problem with our Corporate Communications and Marketing Department is that it is very lousy.

The lack of clear delegation of authority has other serious ramifications. It was found that even the top management of a certain hotel associated the web sites, Intranet and the related organisational trademarks that appear in these sites to be the responsibility of the IT Department. We viewed this to be highly problematic because then these issues are misplaced. This includes the budget thereof.

Legal provision that deals with unsolicited communication has a serious loophole

Unsolicited emails, famously known as spam emails, are addressed in Chapter 7 of the Electronic Communications and Transactions Act No. 25 of 2002. This Chapter of the aforesaid Act deals with consumer protection. The spam emails are dealt with in Clause 45 which prohibits unsolicited commercial communications to the consumers. However, interviewees indicated that this prohibition is not effective. Sellers of the goods, products and services are using a loophole in the Act to send chains of unsolicited messages to the consumers. The Head of Internet Channel in one of the banks noted that:

> The Act says the sender should give the recipient a choice to stop the subscription. However, consumers are uninformed and thus they are swamped with spam emails. In real essence, the first email that is sent is unsolicited, but it is legal because it gives the recipient an option to opt out. Usually, recipients don't opt out and thus the subsequent emails cannot be defined as unsolicited because the consumer is deemed to have opted to receive the adverts since he did not opt out. This is entirely within the law.

The problem is that most banking clients in South Africa have received unsolicited emails which were attached with viruses and spyware. In addition, it was also noted that South African Copyright law is very old; the implementation of the Privacy Bill has been delayed; the patents law is ineffective; and the provisions regarding the prevention of malicious code are difficult to implement.

The level of users' knowledge of information security policies

The word 'user' in this study refers to the information systems users such as employees, independent contractors, service providers, consultants, and all personnel affiliated with third parties who are based in the relevant company. It is therefore imperative for employees to be familiar with the information security policies and, by implication, the legal requirements. It would be a futile exercise for any organisation to have policies that are not known and complied with by the targeted information systems users.

Analysis of the data shows that some users perceive information security policies as a nuisance because they curtail their freedom to certain things in the information systems. Again users feel that effort to acquaint themselves with the policies is time consuming and interferes with the actual work. An Assistant Director who is based in a airliner said:

> I think getting employees to be conversant with information security policies is always a problem because people always feel that security policies get in their way and it's something that hinders them from their work. It is generally difficult to get people to pay attention to policies and all that.

Nevertheless, in some instances, users who are employees familiarise themselves better with policies than users who are customers. This is very prevalent in the banking environment where many Internet Banking holders have been victims of fraud despite the fact that banks have put policies on their websites to assist the users:

> Users who are professionals in their right would be ignorant on basic information security requirements and they lose lots of money due to this. When criminals plunder their accounts they plead ignorance and expect the bank to refund them.

It has been noted that whilst users are knowledgeable with policy aspects such as passwords, acceptable usage of e-mail and Internet, they have rudimentary knowledge of information security issues such as phishing e-mails, pharming websites, and spoofing scams. However, it has also been observed that although policies could have been properly established and approved, the adherence to them is not effective because the only form of awareness is to post policies on the Intranet. A General Manager: Networks in a hotel defended her department regarding the superficial awareness of information security policies:

> It is not our responsibility to train employees; we're IT people. We coordinated the drafting of the policies, forwarded them to a law firm in Cape Town which specialise in IT law, and then got them approved. You are barking up the wrong tree; the culprits in this matter are the HR (Human Resources) guys. HR should do this as part of training, induction, or orientation programmes. The sooner they spend less time training people about dressing and eating etiquette the better.

Even in organisations where the Human Resources Department wants to conduct the awareness programmes, their efforts are usually met by stiff opposition from the ‘core-business’ departments which perceive an information security awareness campaign as a waste of time. The problem is that they cannot link information security and market competitiveness. This is being disingenuous because a company cannot flourish and make lots of money because poor security would lead to huge financial losses and reputational damage.

In some instances, it was found that users are suffering from compliance fatigue. If you mention the word “compliance” to a group of banking, mining, or insurance employees, you may literally see some of them cringing because they are expected to comply with a myriad of laws, regulations, procedures and policies. Although security is highly prioritised in the above-mentioned sectors, information security awareness policies have to compete with other compliance requirements. Problems emanate when the relationship between the employer and employee deteriorates; the user becomes a security risk; that is why in a corporate environment, most information security crimes are committed internally, sometimes with external cooperation. A bitter IT employee may deliberately destroy information systems. When the matter is taken to the Commission for Conciliation, Mediation and Arbitration (CCMA) the estranged employee usually pleads ignorance and the company is blamed for insufficient awareness programmes. Ordinary users may sell information to the company competitors. A Senior Channel Manager: Cellphone & Electronic Channels in one of the big four banks proclaimed:

> You also have users who are honest and genuine employees; their main weakness is gullibility and lack of proper training in terms of security. When such employees are confronted with a ‘social engineer’ they become gullible and fall into the trap; this is very sad. Whilst compliance fatigue is a genuine issue, information security policies awareness should remain on our radar screen.

Information security practitioners have to be creative to gain the attention of the targeted audience. However, one should hasten to indicate that information security policies awareness should not be done in the expense of other compliance requirements.

Conclusions

This study has noted that the participation of the Board of Directors in the provision of information security policies was very minimal; most information security practitioners were not familiar with the legal and policy aspects that they were supposed to integrate in the implementation of information security and thus most organisations were not complying with the law. It has been discovered that there is a general trend in organisations to put low probability to ICT risks and data disaster occurrence. Nevertheless, the reality is that ICT infrastructure is a high risk in itself, and thus a domino effect applies here, as the failure of infrastructure will, without doubt, also lead to the loss of data, information and business intelligence. Organisations cannot continue to perceive the establishment of information security policies, ICT Risk Management Framework and the implementation thereof as a costly overhead which needs to be downgraded. It is therefore critical that organisations integrate legal aspects into information security policies.

The recommendation here is that the governance aspects of ICTs should be taken seriously by the Board of Directors and other governance structures and should not continue to be given less priority due to its technical nature. The alignment of the ICT strategy to the overall business strategy and the impact of ICT in the sustainability of the organisation should be interrogated. The ICT service is vulnerable to failure like any other business function and should also comply with good corporate governance provisions that are contained in the King III Report (2009). According to the legislation, the management of ICT must comply with responsible governance practices where the Board of Directors should exercise its role of being the custodian of corporate governance. In other words, the process of establishing information security policies should be kicked-off by the Board of Directors, up to the auditing and review points.

It is also been noted that the slow implementation of information security laws by the South African government had a negative impact on the corporate environment's attitude towards legislation. Certain provisions in the Electronic Communications and Transactions Act No. 25 of 2002 and the Regulation of Interception of Communications and Provision of Communication-related Act No. 70 of 2002 have not yet been implemented notwithstanding the fact that these two pieces of legislation were promulgated just about ten years ago. It is therefore argued that failure by the government to appear to be taking its laws seriously has negative ramifications on the attitude of corporate South Africa towards information security legislation.

References

Bala, D. (2008). Biometrics and information security. *Proceedings of the 5th annual conference on information security curriculum development*, 64-66.

Beatty, P. Reay, I. Dick, S. & Miller, J. (2011) Consumer trust in e-commerce web sites: A meta-study. *ACM Comput. Surv.* 43(3): 14

Bell, J. (2006). Doing your research project, Fourth Edition, Open University Press, New York.

Bert, J., & Rogers, M. (2004). Social engineering: the forgotten risk In: Tipton, H.F. & Krause, M. eds .(2004). *Information security management handbook*. London Auerbach Publications, 147-154).

Blaxter, L., Hughes, C., &Tight, M. (2010). How to Research, 4th edition. Open University Press, New York.

Bless, C., & Higson-Smith, C (1995). Fundamentals of social research methods: an African perspective. Kenwyn: Juta.

Bond, R. (2002). New economy equity: navigating security and legal issues in digital business. Worcester: John Wiley & Sons.

Braz, F.A., Fernandez, E.B., & VanHilst, M. (2008). Eliciting security requirements through misuse activities. *Proceedings of the 2008 19th International Conference on Database and Expert Systems Application*, 328-333.

Bruns, G., & Huth, M. (2011). Access control via belnap: intuitive, expressive, and analyzable policy composition. *ACM Transactions on Information and System Security*, 14 (1), 9.1-9.27.

Canal, V.A. (2005) On Information Security Paradigms. *The ISSA Journal*. September 2005

Chai, S. Kim, M. & Rao, R. (2010) Firms' information security investment decisions: Stock market evidence of investors' behavior. *Decision Support Systems* 50 (2011) 651–661

Chang, C.Y., Wang, H.J., & Shen, W.C. (2010). Copyright-proving scheme for audio with counter-propagation neural networks. *Digital Signal Processing, 20 (4),* 1087-1101.

Cresswell, J.W. (2007). Qualitative inquiry and research design: choosing among five approaches. Sage Publications: London.

Deane, J.K., Ragsdale, C.T., Rakes, T.R., & Rees, L.P. (2009). Managing supply chain risk and disruption from IT security incidents. *Operations Management Research, 2, 4-12.*

Dey, I. (1993). Qualitative data analysis: a user-friendly guide for social scientists. New York: Routledge.

Dargie, C. (1998). Observation in political research: a qualitative approach. Politics, 18(1), 65-71.

Devers, K.J., & Frankel, R.M. (2000). Study design in qualitative research-2: sampling and data collection. *Education for health: change in learning & practice*, 13(2), 263-271.

Doinea, M. (2009). Open sources security – quality requests. *Open Source Scientific Journal, 1(1), 126-135.*

Dunlop, A.J.S. (2005). South Africa. In: Campbell, D. ed. *E-commerce and the law of digital signatures*. Dobbs Ferry, NY: Oceana, 559-578.

Fenz, S. & Ekelhart, A. (2009) Formalizing information security knowledge ASIACCS '09: *Proceedings of the 2009 ACM symposium on Information, computer and communications security*, ACM, 2009.

Fumey-Nassah, G. (2007). The management of economic ramification of information and network security on an organisation. *Proceedings of the 4th annual conference on information security curriculum development.*

Hanford, M. (2009). Who's who in program management: an overview of roles? G00166959, Gartner Inc., Stanford.

Harris, J. (2003). In praise of unprincipled ethics. *Journal of Medical Ethics*, 29, 303-306.
Henning, E., Van Rensburg, W., & Smit, B. (2004). Finding your way in qualitative research. Pretoria: Van Schaik Publishers.

Institute of Directors in Southern Africa. (2009). King report on governance for South Africa. Johannesburg: IoD.

Johnston, C. & Warkentin, M. (2010) Fear Appeals and Information Security Behaviors: An Empirical study.*MIS Quarterly* Vol. 34 No. *3*, pp. 549-566

Kalof, L., Dan, A., & Dietz, T.(2008). Essentials of Social Research, Open University Press, Berkshire, England, 82-89.

Katz, F.H. (2006). Campus-wide spyware and virus removal as a method of teaching information security. *Proceedings of the 3rd Annual Conference on Information Security Curriculum Development*, 1-4.

Kesh, S., & Ratnasingam, P. (2007). A knowledge architecture for IT security. *Communications of the ACM – Creating a science of games*, 50 (7), 103-108.

Kyobe, M. (2005) Addressing e-crime and computer security issues in homes and small organizations in South Africa. *Proceedings of the Fifth annual ISSA Information Security Conference, South Africa*.

Lamprecht, C. (2004). Hacker risk in e-commerce systems with specific reference to the disclosure of confidential information. *South African Journal of Information Management, 6(4).*

Leedy, P.D., & Ormorod, J.E. (2005). Practical Research: Planning and Design, Seventh Edition, Upper Saddle River, Merill Prentice Hall.

Logan, P.Y., & Clarkson, A. (2005). Teaching students to hack: curriculum issues in information security. *Proceedings of the 36th SIGCSE Technical Symposium on Computer Science Education*, 37(1), 157-161.

Maswera, T., Edwards, J., & Dawson, R. (2009). Recommendations for e-commerce systems in the tourism industry of sub-Saharan Africa. *Telematics and Information, 26, 12-19.*

Maiwald, E. (2004). Fundamentals of network security. New York: McGraw-Hill Technology Education.

Mamaila, K., & Green, J. (2002). Business secrets: SA. Spies take on the world. IOL. Joahannesburg.

Manion. M., & Goodrum, A. (2000). Terrorism or civil disobedience: towards a hacktivist ethic. ACM SIGCAS Computer and Society, 30(2), 14-19.

Merriam, S.B. (1998). Qualitative research & case study applications in education. San Francisco: Jossey-Bass Publishers.

Micco, M., & Rossman, H. (2002). Building a cyberwar lab: lessons learned teaching cybersecurity principles to undergraduates. *Proceedings of the 33rd SIGCSE Technical Symposium on Computer Science Education,* 34(1), 23-27.

Mlangeni, S.A. & Biermann, E. (2005) Assessment of Information Security Policies within the Polokwane Region: A Case Study. *Proceedings of the Fifth annual ISSA Information Security Conference, South Africa*

Nolan, J., & Levesque, M. (2005). Hacking human: data-archaeology and surveillance in social networks. *SIGGROUP Bulletin*, 25(2), 33-79.

Rowlands, B. H. (2005). Grounded in Practice: Using Interpretive Research to Build Theory. *Electronic Journal of Business Research Methodology Volume 3 Issue 1* , 81-92.

Savola, R.M. (2007). Towards a taxonomy for information security metrics. *Proceedings of the 2007 ACM workshop on quality protection,* 28-30.

Schneider, B. (2000). Secrets and lies: digital security in a networked world. New York: John Wiley & Sons.

Sha, W. (2008). Types of structural assurance and their relationships with trusting intentions in business-to-consumer e-commerce. *Electron Markets, 19, 43-54.*

Skoudis, E. (2004). A new breed of hacker tools and defenses (In: Tipton, H.F., & Krause, M. eds. (2004) *Information security management handbook*. London Auerbach Publications, 135-146).

Stoecklin-Serino, C.M. (2009). An examination of the impacts of brand equity, security, and personalization on trust processes in an e-commerce environment. *Journal of Organizational and End User Computing, 21(1).*

Sukhai, N.B. (2004). Hacking and cybercrime. *Proceedings of the 1st Annual Conference on Information Security Curriculum Development*, 128-132.

Summer, M. (2009). Information security threats: a comparative analysis of impact, probability, and preparedness. *Information Systems Management, 26, 2-12*.

Summers, W.C., & Bosworth, E. (2004). Password policy: the good, the bad, and the ugly. *Proceedings of the Winter International Symposium on Information and Communication Technologies*.

Tran, M.Q. (2010). Understanding the influence of 3D virtual worlds on perceptions of 2D e-commerce websites. *Proceedings of the 2nd ACM SIGCHI symposium on engineering interactive computing systems*.

Venter, I. (2005). Cybercrime dot-conned: virtual crimes are very real. *Engineering news*. Gordon View: Creamer Media.

Walliman, N. (2001). Your research project — a step-by-step guide for the first-time researcher. London: SAGE.

Walsham, G. (2006) Doing Interpretive Research. European Journal of Information Systems, 15(3) pp 320-330.

Zhang, Y., Deng, X., Li, Y., Wu, J., Sun, X., & Deng, Y. (2011). E-commerce security assessment under group decision making. *Journal of Information & Computational Science, 8, 7-15.*

APPENDIX G

Paper submitted for publication

Dagada R, and Eloff M.M., (2014), Towards the Development of Concept Model of Legal Compliance for Information Security in the South African Corporate Environment, to be submitted to the *South African Journal of Information Management* (SAJIM).

Towards the Development of a Concept Model of Legal Compliance for Information Security in the South African Corporate Environment

Abstract

Evidence shows that currently there is no concept model to guide corporate South Africa in the implementation of information security within the broader framework of the law. The need for such a model was identified by the main finding of the broader qualitative study of which this paper is part. Forty-five organisations from around the country participated in the study. Analysis of the data showed that there is little participation by the organisations in the provision of the information security policies; most information security practitioners are not familiar with the legal and policy aspects that they are supposed to integrate in the implementation of information security and thus, most organisations were not complying with the law. Nonetheless, this paper will, by proposing a concept model, synthesise legal requirements and information security operational necessities into a single model. The study adopted a hypothetical company in order to demonstrate how the proposed model can be implemented in a corporate environment. Such a study makes a contribution to the body of information security theory and knowledge by a model on how legal requirements are incorporated into the information security endeavours – policy formulation, implementation, monitoring, and evaluation.

Key words: concept model; information security; policy; implementation; corporate environment; legal requirements, policy requirements

1. Introduction

While many South African organisations have adopted e-commerce in their transactions, they may not be immune to risks, threats and crime due to inadequacy in integration and implementation of information security issues (Wu & Ye, 2014). Research shows that companies that succeed in e-commerce are those that implement information security policies (Rastogi & Solms, 2012). However, the internet revolution is developing so rapidly that it remains a challenge to most organisations to remain abreast of developments (Morrison, 2013).

In many organisations, there is a general trend to put low probability to ICT risks and data disaster occurrence (Dagada & Eloff, 2013). The reality is that ICT infrastructure is a high risk in itself, and thus a domino effect applies here, as the failure of infrastructure will, without doubt, also lead to the loss of data, information and business intelligence (Latimer, 2013). Organisations cannot continue to perceive the establishment of information security policies, an ICT Risk Management Framework and the implementation thereof, as a costly overhead which needs to be downgraded (Ahmad, Zuraini, Rahim & Zairah, 2012). According to Trcek and Likar (2014), information security policy is meant to inform all individuals within an organisation regarding their actions in relation to ICT information security issues. Nonetheless, in some settings, policies are drafted because of regulatory requirements (Huber, 2012; Dagada & Mukwevho, 2013). Drafting information security policies just for the sake of satisfying regulatory obligations is not good enough (Bin-Muhaya & Ali-Minhas, 2012).

Literature in South Africa depicted the operational necessity and legislation requirements of the integration of legal aspects to information security policies in various companies (Westby, 2013; Dagada & Eloff, 2013). The evidence shows that currently there is no concept model to guide corporate South Africa to implement information security within the broader framework of the law (Lodi, Anniello, Di Luna & Baldoni, 2014). This paper will, therefore, by presenting a proposed concept model, synthesise legal requirements and information security operational necessities into a single model. This study makes a contribution to the body of information security theory and knowledge. In this model, legal requirements are incorporated into the information security endeavours – policy formulation, implementation, risk management framework, monitoring, and evaluation. This model should be seen as a synthesis of theory, practice and cognitive perspectives gained over the years of research and practical experience of the author. It should however, be stressed that the model developed in this paper is the researcher's conceptualisation of a model which could guide organisations in the country to implement information security in their businesses.

1.1 Research design issues and context

Briefly, the aim of the study is to assess how South African companies integrate legal and policy aspects when dealing with information security issues. In the study, a qualitative research approach embracing semi-structured interviews as well as document and web analysis were used for data gathering. Forty-five organisations from different industrial sectors in South Africa participated in the study. Analysis of the data showed that there is little participation of organisations in the provision of the information security policies. It further shows that many information security practitioners are not familiar with the legal and policy aspects that they are supposed to integrate in the implementation of information security. This means many organisations are not complying with the law. Meta-analysis of the study revealed that both the government and corporate South Africa were not implementing some of the information security legal requirements. However, it is hoped that this model proves to be useful to policy formulators, directors of the boards, ICT executives, and information security practitioners in incorporating/addressing legal requirements in their policy formulation.

The proposed Concept Model combines theory, the author's extensive experience (as an academic and ICT Manager) and cognitive perspectives gained over many years. It should be noted that this study was a product of interplay between the researcher's ontological position and the empirical findings of the study. The author's perspective has influenced the research methodology employed in the study, and, by implication, the findings of the study and the Concept Model. The model was necessitated by the main finding of the broader study of which this paper is part.

In order to demonstrate how the proposed model can be implemented in a corporate environment, the study adopted a hypothetical company named Aifheli Pty Ltd in which the model would be implemented. Aspects related to the model are real whilst the descriptions of the phantom company are simply fictitious, but of significance for illustration purposes. As part of illustrating how the concept model can be implemented, I have dealt with macro and micro aspects of the organisational implementation of the Concept Model of Legal Compliance for the Information Security in the Corporate Environment (CMLCISCE). The macro organisational initiatives are the foundation for the actual implementation of the concept model. These include the establishment and implementation of the ICT Enterprise Architecture; and the implementation. At micro level, the paper demonstrates components of the concept model and roles played by the Board of Dierctors, Group ICT Steering Committee, Group ICT Management Committee, Board of Dierctors' Audit Committee, and all employees involved in the formulation, implementation, monitoring, and evaluation of information security policies.

The proposed concept model will present a structured organization that is generic in its disposition, is product independent and will cater for both sides of information security practice - governance and operations.

1.2 Aifheli Group of Companies

In order to demonstrate how the proposed model can be implemented in a corporate environment, we have decided to construct a hypothetical company (Aifheli Pty Ltd) in which the model would be implemented. Consequently, aspects related to the model are genuine whilst the descriptions of the phantom company are simply fictitious, but of significance for illustration purposes. The Group has four entities (companies) as follows – Aifheli Mines, Aifheli SHERQ (Quality, Safety, Health, and Environment) Solutions, Aifheli HRD (Human Resources Development) Services, and Aifheli Autocatalytic Converter Solutions. Figure 1 (see appendix) illustrates the structure of Aifheli Pty Ltd.

2 The Proposed Model of Legal Compliance

The CMLCISCE will be implemented on macro and micro level. A major difference between macro and micro model implementations is that the macro level deals with overall ICT governance issues, whilst at the micro level, the focus is specifically on the integration of legal aspects in information security policies and the implementation thereof.

2.1 Macro-organisational model implementation

The proposed model cannot be implemented in a vacuum and thus certain ICT macro-organisational initiatives have to happen before the actual implementation. The aforesaid macro-organisational issues include the following – establishment and implementation of the ICT Enterprise Architecture; and implementation of the ICT governance structures.

2.1.1 Establishment and implementation of the ICT Enterprise Architecture

A major concern emerging from the international environment, and South Africa in particular, is that ICT has, in more ways than one, become disconnected from the business and is thus losing touch with the core activities (Jisarek, 2012; Dagada & Eloff, 2013). Whilst a number of reasons are attributable to this state of affairs, the major causal factor is that when major institutions evolve and restructure, they tend to temporarily lose focus. This may result in support functions like ICT assuming a corporate life of their own without necessarily being aligned to the core business of the organisation (ibid). The disconnection between ICT and the business can be resolved by establishing an Enterprise Architecture as part of implementing the proposed Concept Model of Legal Compliance for Information Security within the Group. Aifheli should establish an Enterprise Architecture.

The Enterprise Architecture will provide an organisational model for the deployment of ICT within the company. This Enterprise Architecture, which should be aligned to the company strategy, articulates the required ICT infrastructure and its role in business processes. ICT, in this instance, should not just be seen as a support function, but should play a major role in the core business of the organisation (Cumbie & Sankar, 2012; Dagada & Eloff, 2013). The suggested Enterprise Architecture should, firstly, be positioned and aligned to the four fundamental characteristics of the Aifheli core business (business reality) – Mining, SHERQ, HRD, and autocatalytic converter manufacturing. Secondly, it should cater for operational effectiveness by defining the role of ICT in the Group shared services such as – human resources, marketing, finance, procurement, treasury, legal affairs and auditing; and thirdly, align to the governing aspects that are contained in the organisational vision, mission, and strategy (Stantchev, Petruch & Tamm, 2013).

The Enterprise Architecture should recognise the crucial role of the ICT user in the various entities within the Group in the implementation and the overall management of the ICT infrastructure and applications. The provision of ICT should nevertheless, be aligned to national and international best practices (ibid).

2.1.2 Establishment and implementation of the ICT governance structures

As part of implementing the proposed Concept Model of Legal Compliance for Information Security in the corporate environment, it is suggested that the Aifheli Group should, at the macro-level, have a five tier ICT governance structure.

i. Board of Directors

The Board of Directors is the highest level of the governance in any company. The Board also has fiduciary responsibilities. Between the shareholder's Annual General Meetings (AGMs) of any organisation (Non-Profit Companies, Profit Companies, and Private Companies) the Board of Directors is the uppermost governance structure. This statement is in line with the provisions of the Companies Act, No. 71 of 2008 and the King Report on Governance for South Africa (2009) (commonly known and hereafter as: King III Report, 2009). According to the Companies Act, No. 71 of 2008, the duties of directors caters for both fiduciary responsibility and duty of reasonable care. The implication of this is that the business and activities of an organisation should be conducted under the management or direction of the Board within the powers and authority provided by the aforesaid Act, common law, and other relevant pieces of legislation. In line with the top-down approach, the Board of Directors will make certain broad ICT pronouncements or policy directives that should be established and implemented at an operational level. In other words, the Board of Directors will depart from the concept of the 'bigger picture', the comprehensive position, and most of the time it will serve as the point of departure where ICT policy initiatives are formulated and governed. In terms of the bottom-up approach, the Group ICT Steering Committee will, in line with the legislation and/or company policies, take certain matters to the Board of Directors for information or decision-making purposes. According to this study, the Board should have five sub-committees as follows – audit, nomination and compensation, corporate governance, investment, and sustainable development.

The *Audit Committee*, to be responsible for identifying and mitigating the risks, which includes ICT related risks. The Committee should approve information security policies and monitor compliance; and on behalf of the Board of Directors, determine if the legal aspects have been integrated into information security policies.

The Nomination and Compensation Committee is responsible for advising the Board of Directors regarding people who can serve as either non-executive or executive directors. Due to the pervasiveness of the ICT role within the organisation and the bluring of the boundary between the typical 'business and the 'business of ICT within the organisation', it is advisable for the Nomination and Compensation Committee to ensure that amongst the Non-Executive Directors, there is someone with a broad knowledge of ICT related risks.

The *Corporate Governance Committee* should be responsible for the overall oversight of corporate governance by ensuring that the company's operations are aligned to best corporate governance practice, overseeing the company's governance pronouncements, assessing the independence of the Non-Executive Directors, and establishing the ethical guidelines for directors and measures to deal with conflict of interest.

The *Investment Committee* should advise the company regarding its main strategic thrust. This committee will make recommendations on dealing with organic or/and acquisition growth, disposals, and strategic partnerships.

Sustainable Development Committee: should ensure that the company approaches sustainability in an integrated manner by bringing together economic, environmental and social aspects into the inextricably woven fabric of the Group. This committee should also ensure that its ICT operations do not lead to environmental decay.

ii. Group ICT Steering Committee

This committee should be constituted by all the Executive Directors of the organisation. In the context of the Aifheli Group, members of the Group ICT Steering Committee will be the Group CEO, Group Chief Operations Officer, Group Finance, Group CIO, and the CEOs of the Group's four entities. The Group ICT Steering Committee should be chaired by the Group CEO and an independent Advisor should be appointed to advise the committee. The purpose of this committee is to: –

- ensure that the ICT systems and infrastructure are in place to support the Board in the execution of its responsibilities in terms of good corporate governance, accountability, and business performance;
- ensure that the ICT strategy and all major ICT initiatives are aligned to the company's business goals and success metrics;
- deal with ICT related matters as per the Board of Directors' directives;
- identify ICT priorities against the broad goals of the Group and with the advice from the CEO's of the four entities within Aifheli;
- pay attention to the ICT related risks and governance issues;
- consider the reports from the Group CIO regarding the performance of the ICT function and budgets;
- determine the impact of ICT systems and infrastructure on business processes and performance; assume the highest-level governance role over projects and consider reports of all projects and ICT initiatives in the Group;
- identify major strategic directions and matters with regard to the company's needs in terms of ICT;
- determine, based on proposals presented by the Group CIO, the ICT policy framework and formulate and review the Group ICT programme in relation to all rolling capital projects underpinning the shared services and the core business of the company.

The Steering Committee should meet bi-monthly.

iii. **Group ICT Operations Committee (OpsCom)**

OpsCom members should be made up of CEOs and two General Managers from each of the four entities of the Aifheli Group, the Group CIO, and the Group Chief Operations Officer. OpsCom should be chaired by the Group Chief Operations Officer and should meet once per month. The main purpose of OpsCom is to determine the ICT needs of the Group entities, identify gridlocks in business processes and ensure the effective coordination of the ICT rollout across the entire Group. OpsCom should also establish action plans to enhance the role of ICT in improving operations and pay attention to ICT risks. Appropriate attention should be placed on the deployment of ICT systems and infrastructure and the determination of proper controls to be maintained by each entity over the decentralised ICT systems (Cumps, et al 2003). As part of exercising this responsibility, OpsCom should make sure that all the information security related issues are satisfactorily attended to and resolved. OpsCom should, where necessary, establish working groups and ad hoc subcommittees to deal with specific ICT operational matters. OpsCom should make recommendations to the Group ICT Steering Committee with regard to the ICT investments and operational matters with high impact on business performance.

iv. **ICT Entity Committees**

Each of the entities should have its own ICT committee chaired by the CEO. The Chair should serve on OpsCom. The entity committee should be the main platform in which the voices of users are heard regarding ICT issues within the Group. The committee should submit ICT reports to the OpsCom reflecting each entity's needs and concerns. Other responsibilities of the committee should be to:

- serve as a platform for the departments within the entity to share information about operational issues and how ICT can be an enabler;
- align the entity ICT activities to optimise ICT and determine the alignment with the Group Enterprise Architecture;
- assess the quality of ICT services on a quarterly basis and recommend service levels to the OpsCom;
- provide input to the OpsCom with regard to the crafting and implementation of the ICT plans and policies;
- monitor the ICT related risks within the entity;
- serve as a safety vehicle to ensure there is a watch over ICT related operations and that interventions can be made before crises arise; and

- coordinate the entity's activities regarding ICT and forward issues of interest and concern to the OpsCom.

The ICT Entity Committee will, where necessary, bring matters of concern and interest to the attention of the Group ICT Management Committee.

v. **Group ICT Management Committee**

The Group ICT Management Committee should be chaired by the Group CIO. A possible organisational structure of Aifheli's Group ICT Management should be constituted by the Group CIO and senior members of his office (Finance Manager, Programmes Manager, Project Manager, and an Independent Advisor), and Heads of Strategy and Governance, User Support, Infrastructure and Systems Solutions, and Enterprise Information Architecture. The purpose of the Group ICT Management Committee is to:-

- align the ICT strategy with the overall Group strategy; implement enterprise-wide best practices and monitor trends globally, nationally, and within the Group;
- ensure that ICT initiatives are linked with business priorities;
- assume overall responsibility for the selection, procurement, deployment, support, and maintenance of infrastructure and systems;
- make sure that all ICT initiatives have clear business objectives and success metrics; conduct regular monitoring of the ICT skills of employees on behalf of the entities and the Group;
- make recommendations to the Group ICT Steering Committee regarding the alignment of ICT investments and strategic initiatives and operational needs of the entities and shared services;
- make recommendations to the Group ICT Steering Committee to approve the implementation of large scale ICT programmes and projects;
- establish and deploy a consolidated ICT Service Delivery Model;
- establish and maintain an ICT Disaster Recovery and Business Continuation Plan and Procedure;
- establish and implement draft ICT policies portfolio;
- establish and implement draft ICT standards portfolio;
- establish and implement draft ICT Procedures Portfolio;
- establish and implement draft ICT Risk Management Framework; and
- operationalise and implement decisions taken through approved recommendations and directives from other governance structures.

The next sub-section deals with the micro-organisational model implementation.

2.2 Micro-organisational model implementation

According to the King III Report (2009), enterprise strategic planning, risk management and information security are the primary responsibilities of the Board of Directors. One does not expect the Board of Directors to be involved in a detailed process regarding the formulation of the information security policies, but they should rather make broader pronouncements within the business strategic direction and sustainability, corporate governance, standards, and legislation framework. Other parties (components of the model) that play a role in the formulation, implementation, monitoring and evaluation are the Board of Directors, Group ICT Steering Committee, Group ICT Management Committee, Board of Directors' Audit Committee, and Whole Organisation. Figure 2 (see appendix 1) illustrates the placement of each governance structure in the process of integrating legal aspects in information security policies and their implementation, and the interface between the governance structures. The numbers in the figure shows the steps or sequence of getting the process completed successfully. In the following paragraph, the single digit in brackets shows the step in the process as depicted in Figure 2. Arrows indicated ABCD in the figure show that, in some instances, while following the steps within components of the model, collaboration and/or consultation may be direct between the highest levels/steps and the bottom. For instance, arrow A shows that though the Board's sub-Committee on risk management which is on step 5, can consult directly with the Board of Directors who are on step1.

The King III Report (2009) and Companies Act, No. 71 of 2008 require that a public company like the Aifheli Group should have a Board of Directors as the highest governance structure in the company. The Board of Directors (1) may have committees that serve as working groups focusing on specific governance areas. It is suggested that relevant information security and related compliance duties should be identified at this level. Once this has been done the next governance structure will be the Group ICT Management Committee. The Group CIO, as the chairperson of this committee, should serve on both the Group ICT Steering Committee (2) and the Board of Directors as one of the Executive Directors. This would enable the Group CIO to take the identified information security legal provisions, requirements and related compliance duties and translate them into information security policies. The drafted information security policies will then be taken by the Group ICT Management Committee (3) to the Group ICT Steering Committee (4) for consideration and comment. The Group ICT Steering Committee will allocate duties to the business units and/or individual positions. The policies will then be taken to the Board's sub-Committee on risk management (5) for their approval. All employees (6) will then be trained regarding the information security policies. They will also be asked to sign an Employee Acceptance Form, and the Employee Interception Consent (7). The Audit Committee (8) will assess compliance and identify gaps. Thus the overall intention of the model is the integration of legal aspects in the information security policies' formulation, implementation, monitoring, and evaluation, to elevate the benefits of business security, and ultimately address corporate security lapses.

3. Discussion of the components of the model

3.1 Board of Directors gives directives regarding ICT policies

ICT plays an important role in the functioning of a company and that is why its failure can threaten the sustainability of the organisation (Demirkan & Delen, 2013) and therefore the Board of Directors should articulate broad ICT policy directives. The Board of Directors does not have to get involved in the technical details of such pronouncements.

In its endeavour to conform with legislation, the Board of Directors should be familiar with ICT risks as outlined by the literature, King III Report (2009), and Buys attorneys (2006): liability, risk or harm resulting from employees' abuse of electronic communication; risk resulting from a website and/or E-Commerce; risk resulting from theft of ICT equipment; risk resulting from software risk; and risk presented by the failure of the Board of Directors and/or company executives to deal with information security breaches. The King III Report (2009) and the Companies Act No. 71 of 2008, explicitly allot risk management as part of the Board of Directors responsibilities. Company management is accountable to the Board of Directors for crafting, implementing and monitoring ICT policies in general, and specifically, information security policies. Due to the pervasiveness and the critical role of ICT in the running of the company, part of the responsibilities of the Board of Directors is to educate and acquaint themselves with the ICT risks and how they can be mitigated through the integration of legal aspects in information security policies.

It is the responsibility of the Board of Directors and its various committees to ensure that the Group complies with the legislation of the Republic. It should, nevertheless, be noted that there are several pieces of legislation that have a direct impact on the manner in which information security policies should be crafted and implemented; please also see Table 1. The Board of Directors may require the Group CEO to ensure that the following areas of information security are addressed in terms of policy implementation – hacking, intellectual property, copyright, protection of trademarks, privacy, and patents protection. The reason for the Board of Directors to give this responsibility to the Group CEO is, in real essence, the Board has only one employee – the Group CEO. That is why, if a huge information security incident happens, the Board of Directors will require the Group CEO to account instead of the Group CIO. At the same time, the Group CEO depends on other executives to carry out his/her responsibilities and thus there is a Group ICT Steering Committee.

3.2 Group ICT Steering Committee identifies security areas and instructs the ICT Management Committee to establish an ICT Governance Portfolio

Almost all members of the Group ICT Steering Committee serve on the Board of Directors as executive directors and thus the provisions of the Companies Act No. 71 of 2008 and King III Report (2009) relating to directors responsibilities and liabilities are applicable to them. The new liabilities heaped on directors by the Companies Act No. 71 of 2008, have equated the responsibilities of South Africa's executives with that of their counterparts in the USA, who had to contend with the governance and reporting responsibilities contained in the Sarbanes-Oxley Act of 2002.

In real essence, this is actually the Group Executive, it is just that, in this instance, the agenda of the meetings only focuses on ICT related matters. Once the Board of Directors pronounces certain policy directives, it is the responsibility of the Group ICT Steering Committee to delegate the actualisation of these directives to individuals and/or structures. In this instance, the Group Steering Committee will delegate the responsibility of crafting information security policies to the Group CIO and the Group ICT Management Committee.

The Group ICT Steering Committee should require the Group ICT Management Committee to address information security areas (hacking, intellectual property, copyright, protection of trademarks, privacy, and patents protection) by establishing the ICT Governance Portfolio which is in line with the legislation of the Republic and the best-of-breed nations and international standards.

3.3 Group ICT Management Committee establishes an ICT Governance Portfolio

This committee has to unpack and put in place details regarding the mandate from the Group ICT Steering Committee by delving into the establishment of the ICT Governance Portfolio. The committee should be sensitive to the fact that ICT Governance is a critical component for an effective ICT strategy and function. It is on this basis that ICT Governance should be documented and communicated to the Group to enable full implementation and compliance. A critical element of ICT governance is the accountability in terms of information security. On the other hand, the Group ICT Management Committee should ensure that ICT functions are within a framework of policies and legal aspects. The lack of policies which integrate legal aspects disadvantages a structured growth of the ICT function within a Group and threatens its sustainability. This should be attributed to the fact that the organisation would not be operating in a normalised operating environment. With the exception of polices which integrate policy aspects, ICT Governance should be constituted by the establishment of operating standards, identifying the operational risks, and comprehending the whole notion of quality management and alignment with the critical success factors for ICT initiatives (vision, people, process, and technology). However, this study focuses only on Information Security Policies Portfolio and the Risk Management Framework.

3.3.1 Establishment of an ICT policies portfolio

The Group ICT Management Committee should acknowledge that many pieces of legislation compel all organisations in South Africa, regardless of the method and form of their incorporation or founding, to comply with the provisions of the legislation in terms of the implementation of information security. This requirement is applicable to all companies as defined by the Companies Act, No. 71 of 2008, that is – for profit companies (state owned company, a private company, a personal liability company, and a public company) and not for profit companies.

Then again, the King III Report (2009) argues that information security is a critical component of the overall business and sustainability and thus companies should address information security by addressing confidentiality, integrity, and availability.

The Group ICT Management Committee should take cognisance of the fact that, making-up a predominant part of corporate ICT governance, ICT policies which integrate legal aspects in terms of information security, will guide the Group position on matters which not only pertain to ICT operations. This is because ICT permeates the company at all levels and enables the flow of the business processes. Due to ICT's pervasive nature, employees' work tends to revolve around ICT and in most instances information security and its relevant pieces of legislation are neglected and thus lead to corporate non-compliance. To avoid this, the Group ICT Management Committee must establish an ICT Policies Portfolio by aligning information aspects with the relevant policies and legislation. Table 1 illustrates the aforementioned recommendation.

Table 1: Synopsis of ICT Policies Portfolio

AREA OF INFORMATION SECURITY	RELEVANT POLICY	RELEVANT LEGISLATION
1) Hacking	• Information Security Policy • Data Privacy Policy • Access to Information Security Policy • Interception and Surveillance Policy • Records Management Policy • E-Commerce Policy	• Promotion of Access to Information Act No. 2 of 2000 • Electronic Communications and Transactions Act No. 25 of 2005 • Regulation of Interception of Communications and Provision of Communication-related Matters Act No. 70 2002 • Common law
2) Intellectual Property and Copyright	• Intellectual Property Policy • Information Security Policy • Data Privacy Policy • Plagiarism Policy • Records Management Policy	• Intellectual Property Law Amendment Act No. 38 of 19997 • Copyright Act No. 98 of 1978 • Merchandise Act No. 17 of 1941 • Films and Publications Act No. 65 of 1996 • National Archives and Records Service of South Africa Act No. 43 of 1996 • Promotion of Access to Information Act No. 2 of 2000
3) Protection of trademarks	• Intellectual Property Policy • E-Commerce Policy	• Intellectual Property Law Amendment Act No. 38 of 1997 • Copyright Act of 1978 • Merchandise Act No. 17 of 1941
4) Privacy	• Data Privacy Policy • ICT Acceptable Use Policy • Electronic Communications Policy • Interception and Surveillance Policy	• Constitution of the Republic of South Africa No. 108 of 1996 • Protection of Personal Information Bill No. 9 of 2009
5) Patents protection	• No company had a distinguishing policy on patent rights	• Patents Act No. 57 of 1978 • Note: Only three organisations addressed patent protection as part of their Intellectual Property Policy • Common law • Intellectual Property Rights from Publicly Financed Research and Development Act No. 52 of 2008.

The proposed ICT Policies Portfolio in Table 1 adequately addresses the findings of the research on which this study is based. They also address ICT risks that were listed by Buys Attorneys (2006) as follows: liability, risk or harm resulting from employees abuse of electronic communication; risk resulting from a website and/or E-Commerce; risk resulting from theft of the ICT equipment; risk resulting from software risk; and risk presented by the failure of the Board of Directors and/or company executives to deal with information security breaches. Table 2 demonstrates how risks identified by Buys Attorneys (2006) are addressed in the ICT Policies Portfolio.

Table 2: Accommodation of ICT risks in the ICT Policies Portfolio

AREA OF INFORMATION SECURITY	RELEVANT POLICY	RELEVANT LEGISLATION
1) Hacking (Buys Attorneys: employees risk, E-Commerce risk, risk, & theft)	• Information SPolicy • Data Privacy Policy • Access to Information Security Policy • Interception and Surveillance Policy • Records Management Policy • E-Commerce Policy • Information Security Standards Management Policy • Procedure Development and Management Policy • Quality Management Policy	• Promotion of Access to Information Act No. 2 of 2000 • Electronic Communications and Transactions Act No. 25 of 2005 • Regulation of Interception of Communications and Provision of Communication-related Act No. 70 2002 • Common law
2) Intellectual Property and Copyright (Buys Attorneys: employees risk, E-Commerce risk, risk, & theft)	• Intellectual Property Policy • Information Security Policy • Data Privacy Policy • Plagiarism Policy • Records Management Policy	• Intellectual Property Law Amendment Act No. 38 of 1997 • Copyright Act No. 98 of 1978 • Merchandise Act No. 17 of 1941 • Films and Publications Act No. 65 of 1996 • National Archives and Records Service of South Africa Act No. 43 of 1996 • Promotion of Access to Information Act No. 2 of 2000 • Common law
3) Protection of trademarks (Buys Attorneys: employees risk, E-Commerce risk, risk, & theft)	• Intellectual Property Policy • E-Commerce Policy	• Intellectual Property Law Amendment Act No. 38 of 19997 • Copyright Act of 1978 • Merchandise Act No. 17 of 1941 • Common law
4) Privacy (Buys Attorneys: employees risk, E-Commerce risk, risk, & theft)	• Data Privacy Policy • ICT Acceptable Use Policy • Electronic Communications Policy • Interception and Surveillance Policy • E-Commerce Policy • Information Security Standards Management Policy • Procedures Development and Management Policy • Quality Management Policy	• Constitution of the Republic of South Africa No. 108 of 1996 • Protection of Personal Information Bill No. 9 of 2009 • Common law
5) Patents protection (Buys Attorneys: employees risk, E-Commerce risk, risk, & theft)	• No company had a distinguishing policy on patents rights	• Patents Act No. 57 of 1978 • Notes: Only three organisations addressed patent protection as part of the Intellectual Property Policy • Common law • Intellectual Property Rights from Publicly Financed Research and Development Act No. 52 of 2008.

Buys Attorneys (2006) also mentioned the risk associated with the failure of the Board of Directors and/or the company's management; this has not strictly been addressed in either Tables 1 or 2. However, measures to deal with the negligence of both non-executive and executive directors are sufficiently catered for in the Companies Act No. 71 of 2008 and the provisions of this Act should not necessarily be part of any information security policies. Other than integrating legal aspects to the information security policies, ICT standards should also be integrated into some policies.

3.3.2 Establishment of an ICT Risk Management Framework

Since ICT is pervasive throughout Group entities and is an enabler of the business processes and connected to suppliers and customers, the Group ICT Management Committee should establish measures to mitigate information security threats. These measures should be done in line with the established ICT Portfolio. In essence, the best mechanism to counteract ICT threats is to actually implement the approved policies. At face value, the point I am making sounds obvious, but practically, it is not so apparent. During the fieldwork of this study, I came across some companies that had well-crafted policies which were never implemented and thus there was a huge disjuncture between the policy and the actual implementation of information security. The proposed ICT Risk Management Framework should comprise the standards, procedures, and quality management.

Standards bring stability in the ICT environment and give assurance to the company that their information security implementation has been implemented within the framework of best practice. Due to the fixed nature of the standards, it is advisable that they should be customised for the particular operational environment. However, customisation should not lead to a major departure from the core framework of the standard. Standards should form part of the ICT Risk Framework and consequently ICT Governance, and thus they should be managed centrally as a portfolio. Apart from integrating aspects of standards into various information security policies, the Group ICT Management Committee should develop an Information Security Standards Management Policy and it should deal with the following aspects: information security areas to be standardised, typical detour from standards, motivation and process for customisation, deployment of the standards portfolio, review of standards, Group ICT Management Committee remit and answerability, and non- acquiescence management. The following standards should form part of the ICT Risk Management Framework – ISO 9000/20000 (which relates to quality assurance in project implementation) and ISO38500 (which deals with the corporate governance of ICT).

The Standard Operating Procedures should be part of the ICT Risk Management Framework. In the absence of operational procedures, it would become difficult to monitor information security performance and compliance with the relevant legislation aspects and standards. I therefore propose the establishment of the Procedure Development and Management Policy.

In addition, the Group ICT Management Committee should make sure that quality management is an integral part of information security implementation. The fact that information security deployment conforms to legislation, best-of-breed standards, procedures and quality management, gives certain assurances to the Group Executive and the Board of Directors. A Quality Management Policy should be established and become an integral part of the ICT Management Framework. Once the ICT Polices Portfolio and ICT Risk Management Framework have been established, the Group CIO should, on behalf of the Group ICT Management Committee, submit them to the Group ICT Steering Committee. It is advisable for the Group ICT Management Committee to seek the advice of the Group ICT Operations Committee and the ICT Entity Committee before they are passed to the Group ICT Steering Committee.

3.4 Group ICT Steering Committee endorsement of policies portfolio and risk management framework

If the Group ICT Steering Committee, for whatever reason, does not endorse the Policies Portfolio and Risk Management Framework, they should be taken back to the Group ICT Management Committee for refinement. However, once the ICT Policies Portfolio and ICT Risk Management Framework have been endorsed by the Group ICT Steering Committee, the Group CEO should, on behalf of the Group ICT Steering Committee, submit them to the Audit Committee for approval.

3.5 Board of Directors' Audit Committee approves policies and risk management framework

The Audit Committee should ensure that the ICT Polices Portfolio and ICT Risk Management Framework that have been endorsed by the Group ICT Steering Committee do not leave loopholes that could compromise the performance and sustainability of the organisation. The Audit Committee should satisfy itself that measures to deal with ICT security risks are integrated into the overall company strategy and that various information security policies are aligned with this strategy. Furthermore, information security policies should have integrated relevant legislation provisions. The Audit Committee should also ensure that ICT related risks and security threats are identified and mitigated. The Audit Committee should get the services and advice of an independent ICT Law Firm or auditing company in executing the assessment of information security policies.

The Audit Committee should check whether information security policies have been formulated to deal with risks and potential threats in a way that is commensurate with the organisation's vision, business priorities, and goals. In line with the recommendations of the King III Report (2009), the Audit Committee should determine how information security policies address three areas – confidentiality (protecting sensitive information from unauthorised disclosure), integrity (safeguarding the accuracy of data, information and software), and availability (ensuring that information and vital services are available when needed). During this period of evaluating the policies, the Audit Committee should liaise with the overall Board of Directors for information purposes and the Group ICT Steering Committee to seek clarity and give feedback.

3.6 Group Human Resources conducts employee training

If the Audit Committee is satisfied with the submitted policies, the Group CEO will be informed and the policies will then be implemented in the whole organisation. The Group ICT Operations Committee and ICT Entity Committee should be involved when it comes to the technical aspects of the policies' implementation. The Group CEO will, on behalf of the Group Steering Committee, give a directive to Group Human Resources to conduct training to all staff members in all the Group entities.

When formulating a corporate Information Security Training Programme, Group Human Resources should take into consideration that ICT systems are dependent on employees. This is in line with Cecere and Rochelandet (2013) who argue that information security is more about people's behaviour than anything else. In other words, in a corporate environment, information security is about thwarting employees' intentional and unintentional actions and the harmful implications thereof. In spite of the propaganda from ICT suppliers about the necessity of information security technology, many essential security actions cannot be automated and thus they rely on the correct usage by the employees. This means that companies are reliant on employees to attain a secure ICT environment. Due to the fact that humans are regarded by several authors (Clarke, Hall & Rapanotti, 2013; Stephanou & Dagada, 2009) as the "weakest link" in the security chain, there is a need for Group Human Resources to make sure that staff members are properly trained regarding the correct implementation of, and compliance with, information security policies.

As part of establishing or procuring a corporate Information Security Training Programme, Group Human Resources should take into account that a real threat in terms of ICT systems is that of insiders, employees, and consultants. This is so because these people are permitted to have advantaged access to the ICT systems, and are familiar with internal processes of the Group and possess some technical knowhow. Together these factors present a considerable risk to the company. It is on this premise that information security awareness and training must be conducted to enable employees to comprehend what they must do to enforce security policies and the rationale thereof. This view is supported by authors such as Chou and Cheng (2012).

3.7 All employees accept security policies by signing Consent Forms

Once the awareness and training programmes have been implemented, each staff member should sign the Consent Form and Employee Interception Consent which would enforce employees' adherence to the principles of good corporate governance; conformance to safety and security of the organisations' network; and ensure a secure and healthy working environment. The Consent Form will enable the company to monitor employees' activities related to the use of Group ICT systems when needs be. The company should take into consideration the fact that, in South Africa, employees have the constitutional right to privacy and thus the Consent Form is a correct mechanism to balance information security objectives and the compliance with the Constitution of the Republic of South Africa No. 108 of 1996.

The Consent Form enables the employees to agree to the necessary undertakings. The Consent Forms should be signed by employees who are already within the organisation when information security policies are approved by the Board of Directors or when they are amended. Provisions contained in the Consent Form should be part of the employment agreement for new employees. Group Human Resources, with the guidance of Group Legal Corporate Affairs, should determine steps that have to be taken against employees who refuse to sign the Consent Forms. Such steps should be taken within the framework of acceptable human resources practices and labour related laws of the Republic of South Africa. Once employees have signed the Consent Forms and the policies have been implemented, the next step in the legal compliance chain will be the audit conducted by Board of Directors' Audit Committee.

3.8 The Audit Committee audits adherence to the security policies

Once policies have been implemented, the Group ICT Committee should constantly monitor information security legal compliance. However, the actual audit of compliance should be done by the Audit Committee on behalf of the Board of the Directors because, whilst monitoring is a management issue, auditing is a governance matter. It is advisable for the Audit Committee to get external independent assistance when carrying out the audit. The Audit should look at both the compliance by the employees, and ICT infrastructure and systems.

Regarding human resources' compliance with the information security policies, it may be advisable to take guidance from Midha and Bhattacherjee (2012) who reasoned that employees' policies compliance can be determined by observing their behaviours and attitudes by: conducting password cracking; doing interviews with employees at pause areas in order to obtain anecdotal evidence; tracking the number and nature of incidents reported before and after information security policies were implemented; conducting clean desk audits; determining who has reviewed the policies; and distributing surveys or questionnaires in order to get input from employees. This may include following up to determine what employees remember and what worked.

ICT infrastructure and systems are devised as intrinsic units, but are actually prone to disappoint due to their digital nature, vulnerability to attacks, and their dependency on resources outside the ICT sphere of influence. It is on this premise that the Audit Committee should also audit the ICT infrastructure and systems to ascertain whether they satisfy the requirements of the information security policies and the established Risk Management Framework.

As a starting point, the Audit Committee should assess to what extent the ICT security infrastructure is linked to the enterprise-wide risk management efforts, at the same time considering that ICT risks cannot always be defined based on the parameters articulated on a corporate level. Backups are very important in terms of mitigating ICT risks and information security threats and thus the audit team should test their performance and whether there is some backup off-site and alignment with the business expectations for data recovery capabilities. As part of the audit, an assessment of the Information Technology General Controls (ITGCs) of the Group should be conducted; Table 3 below serves as an example.

Table 3: Scope of the ITGCs in the Management Campus

Objective		Overview of procedures
COSO Components: Those mechanisms that management has implemented, and uses, to manage the day to day activities of the ICT environment		
1.	Adequate policies & procedures exist governing the day to day operations of the ICT domain.	Inspection of policies and understanding of procedures governing: -security administration; -incident monitoring; -change management; -backups; -batch/job processing; etc.
2.	A defined structure exists under which ICT operates.	-confirmation of organisational structure with a focus on understanding reporting structures, responsibilities and on ensuring key functions are segregated; -understanding and validation of key management meetings (including core audit) with a focus on understanding items discussed, and on the nature and format of documentation produced.
3.	An ICT strategy exists governing the short term and long terms goals, and those steps needed to achieve the goals.	Inspection of ICT strategy with a focus on understanding: -short term goals; -long term goals; -alignment with business; and -steps to be taken to achieve goals
Program Change Control: The process whereby changes are made to data, application functionality & reports		
4.	Only authorised individuals have access to migrate changes into production, and these persons are segregated from those responsible for development activities.	-comparison of list of developers with those responsible for, and with access to, migrate changes into production; -validation of listing to ensure all access is authorised, and to ensure that adequate segregation of duties exists between those responsible, and those responsible for migrating changes.
Access to Programs & data: the process around ensuring application & data access is restricted to authorised individuals		
6.	User provisioning processes ensure that only authorised users have access to the applications and databases.	Validation of user provisioning processes with a focus on ensuring: -all new users are approved; -accounts for terminated users are removed in a timely manner; -adequate segregation of duties exists between critical functions; and -regular reviews are performed on users with access to the shared applications and databases.
7.	Production servers are appropriately configured to reduce the risk of unauthorised access to the databases and shared applications.	Review of security configuration for production servers. Review will be performed using proprietary scripts and will include the validation of high risk security configuration. This will include the review of: -audit logging configuration & associated monitoring procedures; -password parameters; -trusts & servers; and -accounts with administrative privileges.
8.	Administrative privileges are restricted to authorised personnel only and all activities performed with these accounts are authorised.	-Validation of persons with administrative access to application, and associated technical platforms; -Review of audit logging/monitoring procedures for users with administrative access.
Computer Operations: The process around ensuing adequate monitoring of the application environment is performed		
9.	Adequate procedures have been implemented to ensure adequate recovery in the event of the disaster.	-Review and validation of backup schedule and associated monitoring; -Inspection of ICT environmental controls, with a focus on understanding mechanisms implementation to control the server environment; -Inspection of Disaster Recovery Plan (DRP), and review of procedures performed by management to ensure that DRP functions effectively.
10.	Production issues are monitored and resolved in a real time manner.	-Review and validation of job schedule and associated monitoring; -Validation of Help Desk monitoring/tracking procedures.

There are several templates of the ITGCs in literature; however the one appearing in Table 2 has been modified to suit the proposed Concept Model of Legal Compliance for Information Security in the Corporate Environment. The purpose of the ITGCs is to firstly, appraise key controls with the ICT general computerised control environment that support reliable and continuous processing of computerised information systems, and secondly, report to the Board of Directors the areas of perceived weakness or areas for improvement in procedure or control. The Board of Directors will delegate audited matters that need attention to the Group ICT Steering Committee for rectification and implementation.

4. Conclusion

The significant point drawn from this study is that the governance aspect of ICTs should be taken seriously by the Board of Directors and other governance structures and should not continue to be given lower priority due to its technical nature. The alignment of the ICT strategy with the overall business strategy and the impact of ICT in the sustainability of the organisation should be interrogated. Notwithstanding, the ICT service is vulnerable to failure like any other business function and should also comply with good corporate governance provisions that are contained in the King III Report (2009). According to the legislation, the management of ICT must comply with responsible governance practices. The Board of Directors should exercise its role of being the custodian of corporate governance. The lack of, or inadequate, ICT security measures constitute poor corporate governance and thus this paper emphasises that the Board of Directors should pay attention to this. The paper also emphasised the role of the independent Audit Committee, which should amongst others, audit the organisation's ICT infrastructure and systems. Such audits will ensure that ICT related policies are well crafted and implemented to mitigate information security risks. According to the proposed model, the process of establishing information security policies should be initiated by the Board of Directors, up to the auditing and review points.

Inasmuch as this paper has been constructed around a hypothetical organisation in which the proposed Concept Model (of Legal Compliance for Information Security in the Corporate Environment) can be implemented, it is the researcher's belief that this model can be implemented in other real companies despite their governance and management structures. The rationale for presenting the model conceptually was the consequence of the appreciation that the Model will not be implementable without its conceptual nature being sculptured. The researcher contributed to information security knowledge and theory by crafting the Concept Model and demonstrating how it can be implemented. The Concept Model came into being by integrating two traditionally foreign concepts – information security and legislation into a single Concept Model. Before the two concepts were integrated in this paper, the literature review and the findings of the bigger research project on which this study is based, provided detailed referencing to enable the reader to appraise himself of the theoretical and real-life grounding of legal aspects and information security.

References

Ahmad, B.S., Zuraini, I., Rahim, A.B., & Zairah, N. (2012). Security effectiveness in health information system: through improving the human factors by education and training. *Australian journal of basic & applied sciences*, 6(12), 226-233.

Bin-Muhaya, F.T., & Ali-Minhas, A. (2012). On the development of comprehensive information security policies for organizations. *International journal of academic research,* 4(1), 16-22.

Buys Attorneys (2006), *ICT risk checklist with legal, IT and corporate governance solutions* (2nd ed). Cape Town: Buys Inc. Attorneys.

Cecere, G., & Rochelandet, F. (2013). Privacy intrusiveness and web audiences: empirical evidence. *Telecommunications policy*, 37(10), 1004-1014.

Chou, W.C., & Cheng, Y.P. (2012). A hybrid MCDM approach for evaluating website quality of professional accounting firms. *Expert systems with applications: an international journal,* 39(3), 2783-2793.

Clarke, M., Hall, J.G., & Rapanotti, L. (2013). Enterprise architecture: a snapshot from practice. International journal of IT / business alignment and governance, 4(1), 1-10.

Cumbie, B.A., & Sankar, C.S. (2012). Choice of governance mechanisms to promote information sharing via boundary objects. *Information systems frontiers*, 14(5), 1079-1094.

Dagada, R. & Eloff, M. 2013, Integration of policy aspects into information security issues in South African organisations. *African Journal of Business Management*, 7(31) , pp. 3069-3077

Dagada, R., & Mukwevho, S. (2013). Industrial Espionage Threats in Corporate South Africa. *CyberSec2013*, 162-169.

Delen, D., & Demirkan, H. (2013). Data, information and analytics as services. *Decision support systems*, 55(1), 359-363.

Huber, M. (2012). Perfect secrecy systems immune to spoofing attacks. *International journal of information security*, 11(4), 281-289.

Jirasek, V. (2012). Practical application of information security models. *Information security technical report*, 17(1-2), 1-8.

King Report on Governance for South Africa (2009). Johannesburg: Institute of Directors Southern Africa.

Latimer, P. (2013). How to ensure disclosure of information in securities markets post-GFC. *Common law world review*, 42(2), 111-136.

Lodi, G., Aniello, L., Di Luna, G., & Baldoni, R. (2014). An event-based platform for collaborative threats detection and monitoring. *Information systems*, 39, 175-195.

Midha, V., & Bhattacherjee, A. (2012). Governance practices and software maintenance: a study of open source projects. *Decision support systems*, 54(1), 23-32.

Morrison, M.I. (2013). The acquisition supply chain and the security of government information technology purchases. *Public contract law journal*, 42(4), 749-749.

Rastogi, R., & Solms, R. (2012). Information security service branding beyond information security awareness. *Journal of systemic, cybernetics & informatics*, 10(6), 54-59.

Republic of South Africa (2008). Companies Act No. 71 of 2008. South Africa. Cape Town: Government Printer.

Republic of South Africa (2008). Constitution of the Republic of South Africa No. 108 of 1996. South Africa. Cape Town: Government Printer.

Republic of South Africa (2008). Copyright Act No. 98 of 1978. South Africa. Cape Town: Government Printer.

Republic of South Africa (2005). Electronic Communications and Transactions Act No. 25 of 2005. Cape Town: Government Printer.

Republic of South Africa (1996). Films and Publications Act No. 65 of 1996. South Africa. Cape Town: Government Printer.

Republic of South Africa (1941). Merchandise Act No. 17 of 1941. Cape Town: Government Printer.

Republic of South Africa (1997). Intellectual Property Law Amendment Act No. 38 of 1997. Cape Town: Government

Republic of South Africa (2000). Promotion of Access to Information Act No. 2 of 2000. Cape Town: Government

Republic of South Africa (2002). Regulation of Interception of Communications and Provision of Communication-related Act No. 70 2002. Cape Town: Government

Stantchev, V., Petruch, K., & Tamm, G. (2013). Assessing and governing IT staff behavior by performance-based simulation. *Computers in Human behaviour*, 29(2), 473-485.

Stephanou, T., & Dagada, R. (2008). The impact of information security awareness training on information security behaviour: the case of further research. *ISSA 2008 Conference*. University of Johannesburg, 2 to 4 July 2008,

Trcek, D., & Likar, B. (2014). Driving information systems security through innovations – first indications. *Cybernetics & Systems*, 45(1), 56-68.

United States of America. Sarbanes-Oxley Act of 2002. Washington DC.

Westby, J.R. (2013). Cybersecurity & law firms: a business risk. *Law practice: the business of practicing law,* 39(4), 46-49.

Wu, K., & Ye, S. (2014). An information security threat assessment model based on Bayesian network and OWA operator. *Applied Mathematics & Information Sciences*, 8(2), 833-838.

Appendix 1

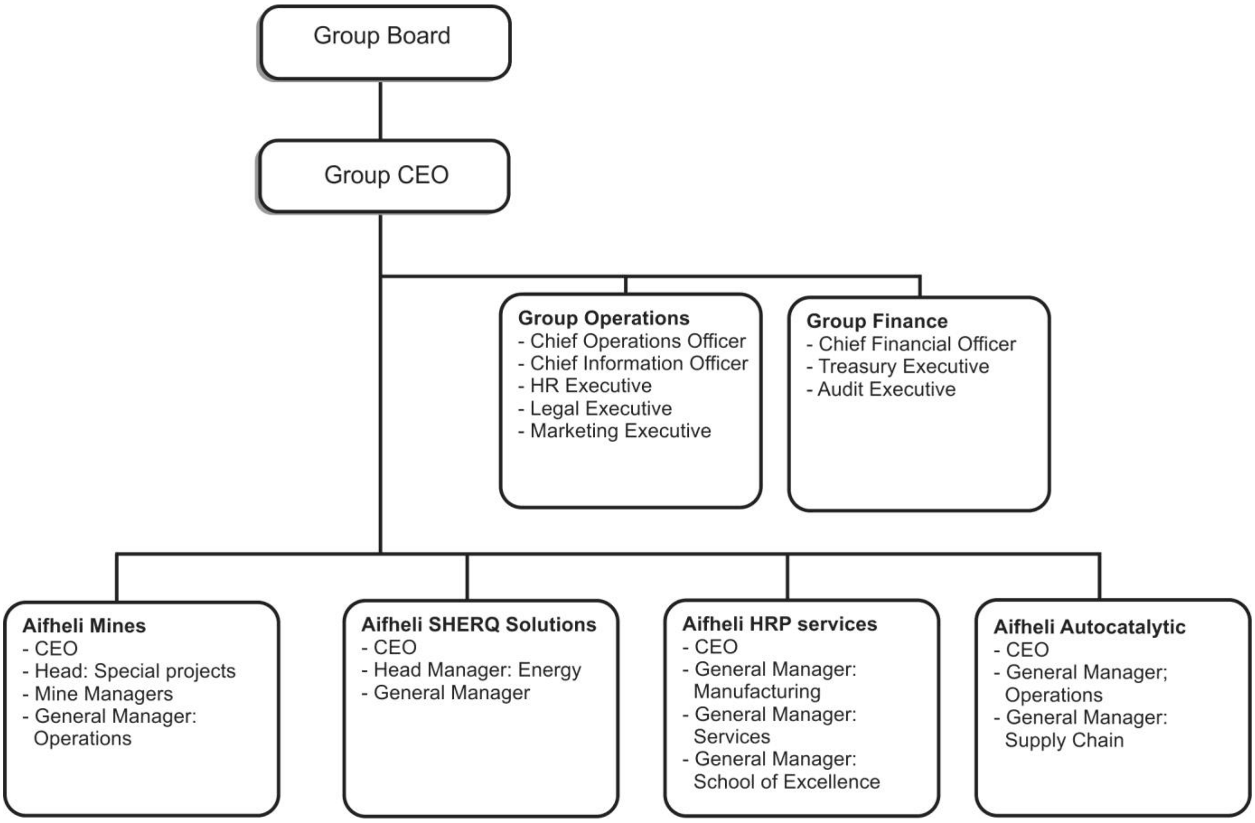


Figure 1: Diagrammatical representation of the structures of Aifheli Group of Companies

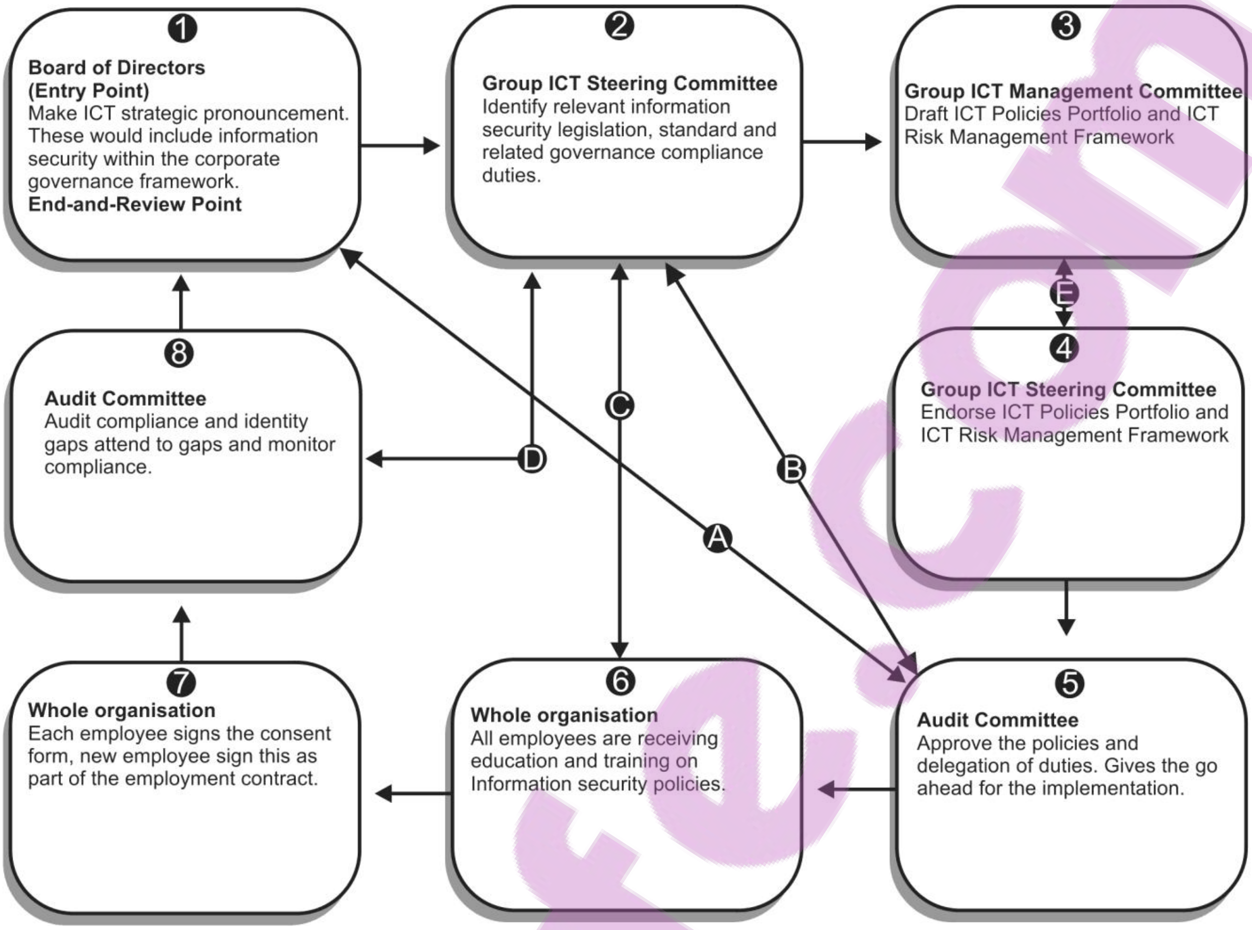

1
Board of Directors
(Entry Point)
Make ICT strategic pronouncement. These would include information security within the corporate governance framework.
End-and-Review Point
2
Group ICT Steering Committee
Identify relevant information security legislation, standard and related governance compliance duties.
3
Group ICT Management Committee
Draft ICT Policies Portfolio and ICT Risk Management Framework
E
4
Group ICT Steering Committee
Endorse ICT Policies Portfolio and ICT Risk Management Framework
8
Audit Committee
Audit compliance and identity gaps attend to gaps and monitor compliance.
D
C
B
A
7
Whole organisation
Each employee signs the consent form, new employee sign this as part of the employment contract.
6
Whole organisation
All employees are receiving education and training on Information security policies.
5
Audit Committee
Approve the policies and delegation of duties. Gives the go ahead for the implementation.

Figure 2: Diagrammatical representation of Concept Model of Legal Compliance for Information Security at Corporate Environment