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

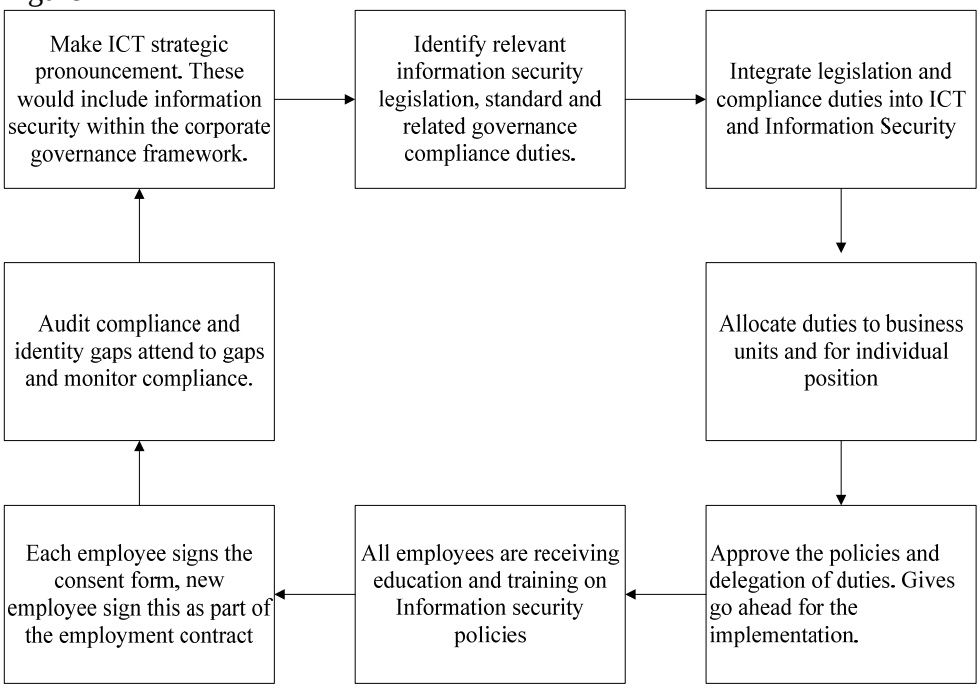

Figure 1: A concept of legal compliance for Information security policies formulation, implementation and multitasking.

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.