# Integration of policy aspects into information security issues in South African organizations

Rabelani Dagada & M.M. Eloff

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 organizations integrate legal and policy aspects when they deal with information security issues. Qualitative research methods were employed to gather and analyses data for the study. Results show that participation by top management in the provision of information security policies is very minimal in organizations. 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 organizations in the country are not complying with the law.

**Key words:** Security risks, South African, organizations, Information Security Policies, legal compliance.

## INTRODUCTION

In South Africa, as in many other countries, many organizations have developed websites for information and business related purposes (Beatty et al., 2011; Bond, 2002). While some of the organizations have their web- sites merely display information about the organization, 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 organization should always be secure. Information Security refers to -measures adopted to prevent the unauthorized use, misuse, modification, or denial 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 (Maiwald,2004). 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 and 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 contextualized corporate description that can enhance the understanding of the intricacies of making use of legislation to improve information security in South African organisations.
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.

## 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 and 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, inadequatell (Kyobe, 2005: 2). Other researchers are also of the opinion that —a sufficiently big set of historic cases must be available for significant probability calculationsll (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 et al., 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 and 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 and 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' pass-words 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-servi*ce 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 and Levesque, 2005:33). This includes the installation of intrusion detection systems to foresee a possible attack (Sukhai, 2004; 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 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 organization'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 prove 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 et al., 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 et al., 2011; Deane et al., 2009).

### Policies and awareness

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 publicized 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 et al., 2008; Devers and 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 organizations 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 et al., 2010; Bless and 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 (W alliman, 2001; Blaxter et al., 2010).The study satisfied the principle of triangulation by employing multiple data-gathering methods and sources (Maswera et al.,2009;W alsham, 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. Wwebsites analysis was used as a data collection method to determine websites' legal compliance. This was achieved by analyzing the websites of all organizations 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 analyzed. 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 analyzed using open coding (Cresswell, 2007). A frequent comparative method was applied to analyses data within and between interviews (Merriam, 1998; Henning et al., 2004). The process involved going through the interview data while marking important sections and adding code to it. While continuing with the process of analyzing 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 analyses 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 analyzed with the intention to distinguish common patterns and to put together categories; these was weighed against the literature and legislation (Leedy and Ormorod,2005; Bell, 2006). Data collected through document analysis was analyzed by comparing it with the South African legal framework pertaining to information security. Content analysis was also used to analyses 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 and 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 organizational 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 organizations 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 DISCUSSION

Data analysis yielded three main themes, namely: the attitude of corporate South African towards information security legislation; the manner in which organizations 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 organizations 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 organizations 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 organizations 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 organizations 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 characterized 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 min to two hours. It doesn't matter where it sits in the world.

Banks are also available 24 h 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 organizations 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 organizations 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 organizational 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 organization 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 an 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 familiarize 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 causal link between them and how they impacted the provision of information security 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 specialize 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 organizations 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 prioritized 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. hilst 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.

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 specialize 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 compliancell 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 prioritized 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 organizations were not complying with the law. It has been discovered that there is a general trend in organizations 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. Organizations 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 organizations 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 organization 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 technologies. According to Skoudis (2004), Savola (2007), the information security staff should occasionally run a password-cracking tool against their users' pass- words 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-servi*ce 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 and Levesque, 2005:33). This includes the installation of intrusion detection systems to foresee a possible attack (Sukhai, 2004; 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 organization'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 prove 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 et al., 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 et al., 2011; Deane et al., 2009).

## REFERENCES


Bala D (2008). Biometrics and information security. *Proceedings of the 5th annual conference on information security curriculum development*, pp. 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 FA, Fernandez EB, 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 VA (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 CY, Wang HJ, Shen WC (2010). Copyright-proving scheme for audio with counter-propagation neural networks. *Digital Signal Processing, 20 (4),* 1087-1101.

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

Deane JK, Ragsdale CT, Rakes TR, Rees LP (2009). Managing supply chain risk and disruption from IT security incidents. Oper. Manage. Res., *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 KJ, Frankel RM(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 AJS (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 organization. *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.

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 FH (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* J. Inf. Manage., 6(4).

Leedy PD, Ormorod JE (2005). Practical Research: Planning and Design, Seventh Edition, Upper Saddle River, Merill Prentice Hall.

Logan PY, 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.

Manion M, Goodrun A (2000). Terrorism or civil disobedience: towards a hacktivist ethic. *ACM SIGCAS Computer and Society*, 30(2), 14-19.

Merriam SB (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 SA, 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 BH (2005). Grounded in Practice: Using Interpretive Research to Build Theory. Electronic J. Bus. Res. Methodology 3(1): 81-92.

Savola RM (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, pp. 135-146.

Stoecklin-Serino CM (2009). An examination of the impacts of brand equity, security, and personalization on trust processes in an e-commerce environment. J. Organ. End User Comput., 21(1).

Sukhai NB (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. Inf. Syst. Manage., 26, 2-12.

Summers WC, Bosworth E (2004). Password policy: the good, the bad, and the ugly. *Proceedings of the Winter International Symposium on Information and Communication Technologies*.

Tran MQ (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*.
Institute of Directors in Southern Africa (2009). King report on governance for South Africa. Johannesburg: IoD.

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. Eur. J. Inf. Syst., 15(3):320-330.

Zhang Y, Deng X, Li Y, Wu J, Sun X, Deng Y (2011). E-commerce security assessment under group decision making. J. Inf. Comput. Sci., 8, 7-15.