# Information Systems Security Practices in South African Small And Medium Enterprises (SME's)

Kishore Singh, Griffith University, Australia

## ABSTRACT

Information systems security is rapidly becoming a growing concern for businesses of all sizes. As security threats and incidents become more pervasive and the legal and business stakes for information security increases, understanding an organization's information security practices becomes essential in the security planning and development process. The purpose of this article is to describe the effectiveness of information systems security practices in small and medium enterprises. To date there is no quantitative or qualitative data within the extant literature describing the state of information systems security practices in small businesses. The data that exists has been produced by commercial organizations with business interests in information systems security consulting or services, such as Deloitte & Touche and Ernst & Young, and by organisations with charter responsibilities in the information security and technology arena, such as the Computer Security Institute. The aim of this study is to contribute to the theoretical understanding of how information systems security should be pursued in small businesses and to provide evidence to assist in the development of policies, programs, and technology in support of information systems security goals in small businesses.

***Keywords***：Information systems security, small businesses, security investment, security management

## INTRODUCTION

The management of information systems security and security related events has become an issue commanding ever-increasing attention from the various professions attending to the information needs of organisations using ICT[i] (von Solms, 2001). The basic need of developing secure information systems (IS), however, continues to remain unfulfilled. This is because the focus continues to remain on the means of delivery of information, i.e. the technology (Galliers, 1993). Management continues to believe that information security and related problems can be solved by technical means (Vermeulen & von Solms, 2002). The responsibility of information security is entrusted to the technical department without proper, direct and continuous support from executive management. The net result is that technology is used to solve the information security problem without a total, comprehensive solution (von Solms & von Solms, 2004).

In this study we define the contribution made by SME's to the South African economy and determine the state of information systems security practices therein. Organisations include businesses as described in the National Small Business Act (NSBA, 1996). This study examines various aspects of information security in SME's viz.: the level of awareness of information security risks, the level of concern regarding security related issues and incidents, security events that are of greatest concern, and key factors that contribute to a reduction in information security risks. South Africa has a thriving small business sector supported by a network of financial and non-financial service providers. By enabling people to meet their basic needs for survival, small businesses play an important role in economic development. It has been proven in many parts of the world that the small business sector stimulates economic growth, redistributes wealth and creates jobs. The latter being particularly important within the context of the reality that large corporations' demand for labour does not increase in proportion to their growth (Ntsika, 2002). A key objective of this study is to develop academic theory regarding the practice of information systems security in small businesses. A secondary objective is the development of a set of management guidelines regarding information systems security policy for small businesses.

The paper is organised as follows: section 2 reviews the related literature and key aspects of information systems security relevant to small businesses are discussed. In section 3 a definition and profile of the SME sector in South Africa is presented. Section 4 provides results of findings of several information security surveys and section 5 provides recommendations for implementing information systems security. Finally we offer some concluding remarks.

## RELATED LITERATURE

NIST (1995:5) defines information security as "the protection of information system assets (including hardware, software, firmware, information/data and telecommunications) against various

[i] ICT (Information & Communications Technology) represents all application and support systems *including* computer hardware, software and communications networks.

threats and attacks in order to preserve the integrity, availability and confidentiality of these systems." Security related problems occur because of the need to balance two important yet conflicting goals viz. 1) the goal of providing access to resources, and 2) the goal of preserving confidentiality, integrity and availability (Mehta & George, 2001).

COBIT (2014) defines ICT is an integral part of everyday business and private life, and dependency on information systems is constantly growing. Emerging technologies allow unprecedented functionality but introduce new risks and environments that are harder to control (e.g. wireless technology, mobile computing and integration of technologies i.e. multimedia). Increased dependency on ICT by individuals and organisations alike implies that the impact of system failures is magnified. Whether the incident happens to a home user (e.g. relying on online banking) or an enterprise (e.g. relying on online customers), security incidents have a real impact. With the proliferation of communication networks, individuals are justified in being concerned about the privacy of their personal information and organisations need to protect the confidentiality of corporate data, while promoting electronic business (COBIT, 2014).

New technology provides the potential for dramatically enhanced business performance hence, improved and demonstrated information security can add real value to any organisation (small or large) by contributing to interaction with trading partners, closer customer relationships, improved competitive advantage and protected reputation. Technology also enables new and easier ways to process electronic transactions and generate trust (ITGI, 2001). However, the resulting increase in technical complexity has led to new and more complex risks (COBIT, 2014).

Blatchford (1998) notes that severe business uncertainty can result from systems that are vulnerable and that poor information security can have adverse economic impacts on individuals, organisations and society in general. Von Solms (1996) suggests that a stage is being reached where an organisations potential business partners will require proof of adequate information security. Failure to provide such evidence may result in the inability to attract new business and the potential loss of some existing business partners. Mitchell ***et.al.*** (1999) confirms this by stating that information security breaches can have a devastating effect on an organisation.

**Threats and Vulnerabilities**

Information systems are susceptible to many threats and vulnerabilities that can cause various types of damage resulting in significant losses. The effects of these threats vary considerably: some affect the confidentiality or integrity of information while others affect the availability of a system (NIST, 1995). In determining the likelihood of a threat, one must consider threat-sources, potential vulnerabilities and existing controls (Stoneburner ***et.al.***, 2002). A threat-source does not present a risk when there is no vulnerability that can be exercised therefore, protection should be provided against threats that can exploit vulnerabilities.

**Information Security Investment**

The concept of investment has one purpose and that is to generate a return. This return is seen in the form of capital, time and both tangible and intangible benefits. Prior to making information security investment decisions, facts about assets (i.e. information, software, hardware and systems), vulnerabilities and the probability of breaches (and damages) need to be analysed. An evaluation needs to be done in order to find the best possible security solution (Tsiakis & Stephanides, 2005).

A key factor in getting value from security is to ensure that technology investments protect the right assets. The financial returns gained from a successful implementation of security should justify the cost of security in terms of enabling the business. An organisation needs to assess security investment against the probability that a loss producing security incident will occur and the consequences of non-implementation of adequate security measures (Tsiakis & Stephanides, 2005; Pipkin, 2000). Gordon & Loeb (2002) proposed a model to determine the optimal amount an organisation should invest in information security mechanisms. In their model the amount to invest in security is taken as an increasing function of the level of vulnerability of the information being protected. However, they propose that the optimal amount to invest in information security should not exceed 37% of the expected loss due to the breach.

Managers responsible for information security are increasingly required to justify their budget requests in purely economic terms. There has been a growing interest in using financial metrics to justify and evaluate investments in information security. According to the CSI (2004) survey, 55% of organizations use ROI (Return on Investment) as a metric, 28% use IRR (Internal Rate of Return) and 25% use NPV (Nett Present Value).

**Impact of Security Breaches**

No information security breach is good, but the impact of some incidents is considerably worse and more difficult to measure than that of others. There's always some financial aspect to security related incidents and organisations intent on not being victimised must pay a price as information security measures come at a price (Gordon & Richardson, 2004).

Every organisation (small or large) must understand the costs associated when information security is breached. Farahmand *et.al.* (2003) notes that the cost of an information security incident must be measured in terms of the impact on the business and, identical incidents in different organisations of the same industry could have different costs. The impact may be financial, in the form of immediate costs and losses, but the more serious incidents are those that have hidden costs associated with them (e.g. loss of brand image, public reputation, goodwill in the market place, and customer confidence).

Studies done by Campbell *et.al.* (2003) and Cavusoglu (2002) provide evidence of an overall negative market reaction to announcements of information security breaches. These announcements also appear to affect the future economic performance of the affected organisations. Garg *et.al.* (2003), conducted a study that extended to include investor reactions to information security incidents on security vendors. They concluded that the share price of security vendors responded positively to information security breaches. This is mainly due to the perception of investors that attacks would result in an overall increase in security spending by all organisations (and not just the affected ones).

**Information Systems Security Management**

A fundamental issue that arises in discussions about information security is that of responsibility. A reasonable answer is that information security ought to be the responsibility of anyone who can affect the security of the system although specific duties and responsibilities of individuals and business units may vary (NIST, 1995).

Birman (2002) states that information security is more than a technical issue, and could even have strategic as well as legal implications. It is therefore important that information security is evaluated at management level and is integrated into the processes of the business. Management involvement is crucial as they are ultimately responsible to the shareholders, and for compliance with applicable laws and regulations (von Solms, 1996; Posthumus & von Solms, 2004).

Straub & Welke (1998) declares that information security continues to be ignored by executive management and, despite the seriousness of risk from security breaches, many organisations are either completely or insufficiently protected. Goodhue & Straub (1991) notes that managerial concern about information security is a function of factors such as: the risk inherent in the industry, the extent of the effort already taken to control these risks, and awareness of previous system breaches. A study conducted by Mitchell *et.al.* (1999), determined that in most organisations the management of information security continues to be placed within the IT function. Furthermore, the study highlights that information security is viewed as a technology problem to be dealt with by the technology staff. This attitude towards information security may contribute to gaps in an organisations chain of defences.

## SME PROFILE

South Africa has a thriving small business sector supported by a network of financial and non-financial service providers. By enabling people to meet their basic needs for survival, SME's play an important role in economic development. It has been proven in many parts of the world that the SME sector stimulates economic growth, redistributes wealth and creates jobs. The latter being particularly important within the context of the reality that large corporations' demand for labour does not increase in proportion to their growth. Furthermore, SME's can easily absorb excess labour capacity, create competitive markets, easily adapt to changing consumer behaviour, provide opportunities for entrepreneurs, easily facilitate on the job training, and play an important role in innovation (Ntsika, 2012).

Enterprises in South Africa are categorised according to the definitions provided in the National Small Business Act (NSBA, 1996). Table 1 summarises the NSBA (1996) classification of small businesses.

**Table 1**. Classification of Small Businesses

| Category | Characteristic |
|---|---|
| Survivalist | income generated is less than the poverty line, there are no paid employees and the asset value is minimal |
| Micro | turnover is less than the VAT registration limit, they are not formally registered and employ between 1- 4 people, excluding the entrepreneur |
| Very small | operate in the formal market and have access to modern technology |
| Small | a secondary co-ordinating management structure is in place with some form of managerial level coordination |
| Medium | further decentralization of decision-making, a more complex management structure and further division of labour are evident |

Source: Adapted from the National Small Business Act 1996

The National Small Business Act (NSBA, 1996:34) additionally distinguishes a small business using the following three criteria: 1) total full-time equivalent employees (<100, with the exception of mining and quarrying; and manufacturing (<200), 2) total annual paid turnover (figures vary according to sector), and 3) total gross asset value (figures vary according to sector).

South Africa's small business sector is the backbone of the national economy and currently employs over 50% of the workforce and accounts for over 35% of the GDP (Ntsika, 2012). According to Ntsika (2012); the contribution of small businesses in 2011 to GDP was 36.1%, up from 32.7% in 2005. Small businesses accounted for at least half of GDP in the agricultural and construction sectors and more than 40% of GDP in the trade, catering and accommodation, as well as the transport, storage and communication sectors.

In 2012, small businesses employed 68.2% of people employed in the private sector, as opposed to 44% in 1995 and 53.9% in 2001. Small enterprises constituted the most significant small business employer, (accounting for 21% of total small business employment), followed by medium-sized (18% of total small business employment) enterprises and micro enterprises (17% of total small business employment).

The largest provinces in economic terms are Gauteng, Kwazulu-Natal and Western Cape, which jointly account for 69% of South Africa's GDP. Some 60% of all enterprises and 70% of all small businesses are concentrated in these three provinces. Small business distribution in these three provinces are; Gauteng (38.4%), Kwazulu-Natal (18.4%) and the Western Cape (13.4%) (Ntsika, 2012).

**SME'S and Technology**

According to Pratt (2002), small businesses have benefited from new technologies that have decentralized computing and telecommunications. In the past only large corporations could acquire the sizable capital required for commerce that depended upon mainframe computers and other costly business equipment. However, since the 1980's the advent of inexpensive personal computers have enabled small firms to compete with larger businesses. First, the cost of equipping a home office has dropped significantly and the capabilities of business tools have improved. Second, the Internet, is transforming the way people work, live and conduct business. E-mail, the Internet and the cell phone offer connections that extend globally from any location - an office building, a home office, a car or boat (for example, Amazon.com, initially started out in a home basement, has since taken over the online book market from Barnes and Noble). Individuals now have access to information and to markets on a 24x7 basis (Pratt, 2002).

Petkov *et. al*. (2003) states that small businesses need technology in order to succeed. Some of these technologies are used to solve the problems of small businesses and to accumulate knowledge for improvement of their services. Lubbe (2004), states that investment in IT has a significant impact on the competitiveness of small and medium businesses. As a result, SME's are beginning to spend a higher percentage of their turnover on technology.

ICT adoption and an Internet presence are emerging as powerful tools for business success. As more small businesses show successful use of ICT, other small businesses will be motivated to adopt these technologies and practices. Embracing ICT and the Internet are critical factors that will determine a small businesses market share in the future. Those small businesses that ignore or hesitate to implement new technologies will be doing so at their own risk (Pratt, 2002).

**SME'S and Crime**

Berger (1981) affirms that security, in general, is a problem for small businesses. A small business does not have the business base across which to spread the cost of security personnel or technologies. Additionally, he concludes that businesses with more than 100 employees are better able to afford a security officer or manager on staff. According to Chelimsky *et.al.* (1981), insurance companies attribute approximately 30% of business failures to internal theft. A twenty year old analysis of white collar crime conducted by Berger (1981) confirms that internal theft by employees surpasses the incidents of shoplifting, hold-ups, and burglary collectively.

Small businesses continue to embrace new technologies resulting in the computerization of many business processes (Pratt, 2002). As a result they have become potentially more vulnerable to internal theft. This is particularly true with regards to theft of money, which is the most threatening crime to small business (Doney, 1998). Most small businesses aren't large enough to have security experts on staff (Keogh, 1981), yet the potential result of computer-based crime can be catastrophic (e.g. business failure, financial and personal liability). Studies described in Doney (1998) indicate that the average loss experienced by a business is about ten times higher when a crime is committed with the assistance of a computer as compared to when committed without it.

According to Pratt (2002), the issues that arise in the move of small businesses to electronic commerce include the cost of establishing and maintaining an Internet presence and security issues associated with on-line transactions. Of the security-related concerns, the predominant one is that of fraud. The concern over fraud is expected to be amplified by security concerns related to digital cash,

as that medium becomes common.

Most small businesses are managed by the owner with only basic management structures (if any) in place (NSBA, 1996). A survey conducted by Lubbe (2004) established that one-half of small business owners do not have any idea of what ICT entails nor how it should be used. It is therefore a reasonable conclusion that by embracing new technologies without correct investigation, implementation or incomplete understanding of the technology itself, small business owners are exposing themselves to a risk environment and are unable to set up and maintain a suitable level of information security without expert assistance. Additionally, PwC (2014a) established that, more than 60% of businesses in the United Kingdom think that information security incidents will continue to increase in the future, despite their high confidence in existing security controls. How then can small business practitioners deal with the ever increasing threat to information security?

Initial attacks of computer-based information systems were aimed at specific organisations, primarily large corporate enterprises. Although smaller firms were attacked, most small firms could somewhat depend on "security through obscurity" (Panko, 2004:10). Today, most attacks are equivalent of firing guns into the crowds. This implies that every computer attached to a telecommunications network has an equal opportunity of being compromised (Panko, 2004).

Lubbe (2004) verifies that a security gap exists between current and required security practices in small businesses. This gap is a result of the absence of a shared vision as there is agreement between large and small business respondents about the importance of certain security tasks and security skills. However, many of these security tasks receive low importance scores from small business practitioners (Lubbe, 2004).

## RESULTS

An analysis of several of the more recent information security surveys (2006 to 2014) were conducted to determine the state of information security in both small & large organisations (Table 2). The results of this analysis reveal that: 1) small businesses represent a very small fraction of organisations surveyed; 2) in general, information security breaches are increasing; 3) there in a significant monetary loss resulting from information security breaches; and 4) the top five most important security concerns are viruses, denial-of-service, some form of theft (ranging from data to equipment), misuse of systems and unauthorised access (hacking).

**Table 2**. Information security surveys

| Survey | Description |
|---|---|
| AusCERT 2006 | 2006 Australian Computer Crime and Security Survey |
| NZ 2010 | 2010 New Zealand computer crime and security survey |
| CSI 2011 | 2010/2011 Computer Crime and Security Survey |
| Cert 2013 | Cyber Crime and Security Survey Report 2013 |
| Deloitte 2013 | 2013 TMT Global Security Study |
| Norton 2013 | 2013 Norton Report |
| PwC 2014a | 2014 Information Security Breaches Survey |
| PwC 2014b | BIS Cyber Security Breaches Survey 2014 |
| EY 2014 | EY's Global Information Security Survey 2014 |
| PwC 2015 | The Global State of Information Security Survey 2015 |

Globally, governments and the private sector are taking cyber security increasingly seriously. PwC's Global State of Information Security Survey (PwC, 2015) found that while organisations are spending more on security, cyber criminals continue to escalate the intensity of their attacks. Detected security incidents had increased 25% over the previous year, while the average financial costs of incidents rose 18% despite overall spending on security increasing by 51% more than the previous year. Data from other information security surveys is given in Table 3.

**Table 3**. Information security survey comparison

| Survey | % Experienced Breach | Loss Value |
|---|---|---|
| AusCERT 2006 | 20% | $48 million (total) |
| NZ 2010 | 28% | $15k /incident (avg.) |
| CSI 2011 | 41% | $100k /incident (avg.) |
| Cert 2013 | 56% | not reported |
| Deloitte 2013 | 59% | $ value not reported, however<br>12% high impact<br>58% medium impact<br>30% low impact |

| Survey | % Experienced Breach | Loss Value |
|---|---|---|
| Norton 2013 | 46% | $110 billion (total) |
| PwC 2014a | 81% (large org.)<br>60% (small org.) | $950k-$1.8m (avg.)<br>$102k-180k (avg.) |
| PwC 2014b | 48% | not reported |
| EY 2014 | 56% | not reported |
| PwC 2015 | 53% | $43 million |

Within the South African context, cyber-attacks are a growing risk to business, but neither the government nor the private sector taking sufficient action to combat it (Jones, 2014). The problem is exacerbated by a shortage of skills combined with a lack of urgency in implementing measures to tackle cybercrime due to South Africa ranking low on a number of cyber security assessments. In the long run, cybercrime will have a negative effect on the country's productivity, national security and its attraction as an investment environment. No comparable survey data exists that uniquely profiles the entire spectrum of South African businesses. However, in the first ever Business Continuity Management Survey ZA (BCMS, 2003) conducted by KMPG and BMI-TechKnowledge, 74% of the respondents indicated that their biggest concern was information security breaches. It must, however, be noted that this survey only sampled South African businesses with an annual turnover of between R100 million to R30 billion. The Norton Report (2013) found that South Africa has the third-highest number of cybercrime victims, after Russia and China. Furthermore, the country does not have a national response team to co-ordinate a cyber-defence strategy, consequently strategic infrastructure, such as aviation or financial systems, may be defenceless when threatened by a cyber-attack. Figure 1 shows the types of violations in information security that occurred (Cert, 2013) while figure 2 provides further evidence of the problem (PwC, 2014b)

Statistics from several surveys (Table 2) confirm that information security breaches continue to rise annually. Furthermore, information security continues to remain a problem for many organisations (small and large), and the provision of effective information security is essential for an organisations continued existence. As more organisations continue to suffer from information security incidents and the associated financial losses, understanding the information security problem becomes essential in security planning and development of effective information security, especially for small businesses.

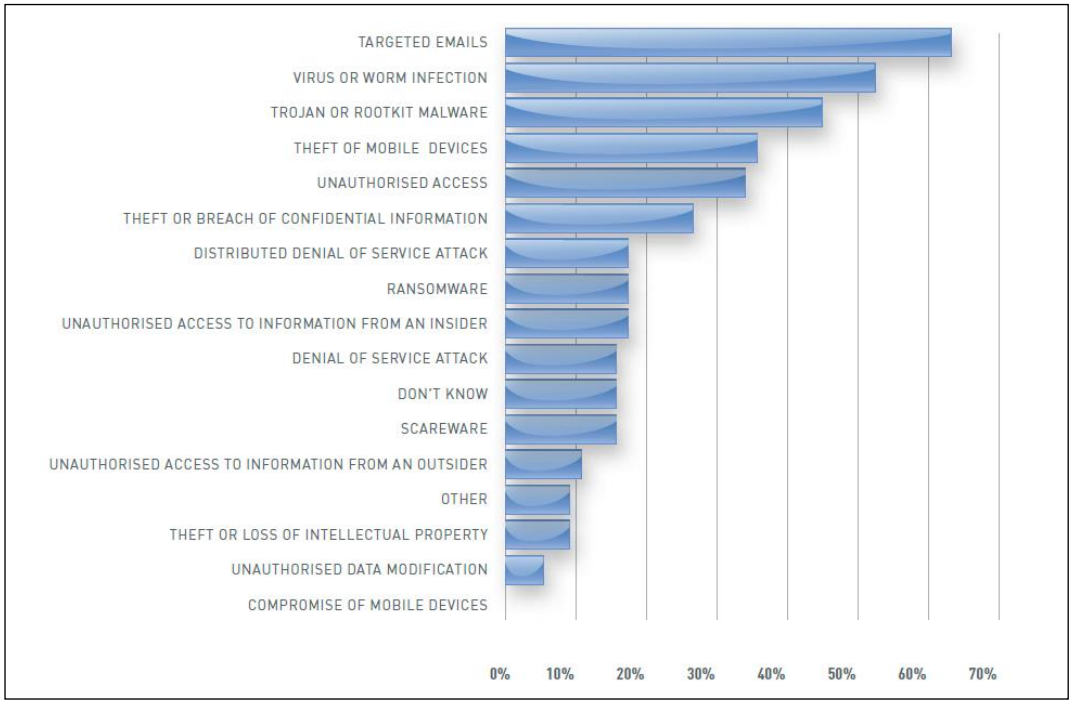


**Figure 1.** Breakdown of types of security events
Source: Cert (2013)

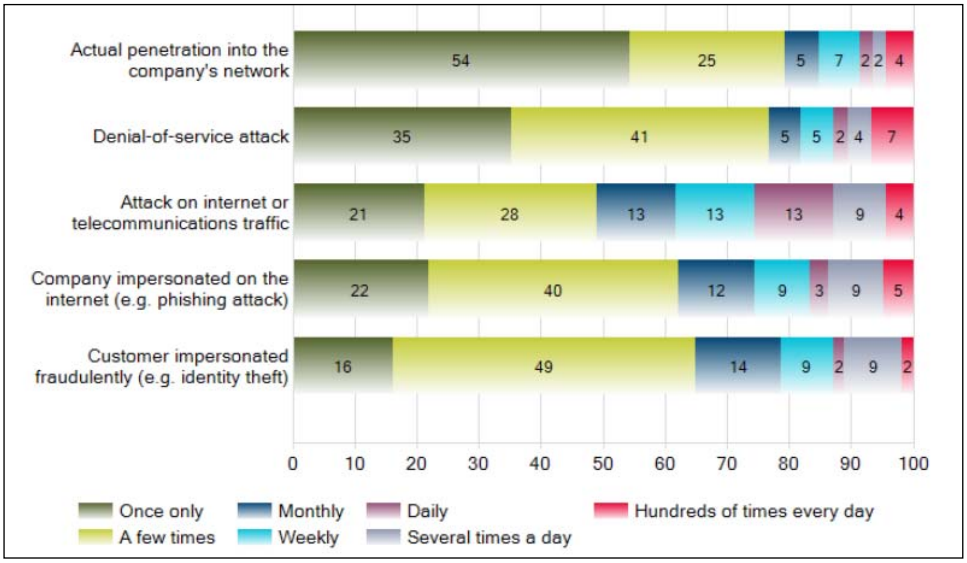


**Figure 2**. Unauthorized outsider attacks
Source: PwC (2014b)

## RECOMMENDATIONS FOR IMPLEMENTING INFORMATION SYSTEMS SECURITY

As organisations develop, previous methods of communication can become less effective. Informal understandings and discussions can prove insufficient. Legal and regulatory pressures increase as companies expand. Providing the entire company with clear, concise, internal governance can bring real benefits in terms of efficiency as well as a means of reducing information risk (DTI, 2014). A policy is an expression of intent. An information systems security policy must provide clear direction and be supported by management for the implementation and maintenance of information security. To be effective the policy must be relevant, accessible and understandable to all intended users throughout the organisation (DTI, 2014).

An information systems security policy is an important document to develop while designing an information system (Lichtenstein, 1997; WatchGuard, 2014; DTI, 2014; Microsoft, 2014). It is essential that the security policy establishes an organization's basic commitment to information security, formulated as a general policy statement. The policy is then applied to all aspects of the system design or security solution. It identifies security goals (for example. confidentiality, integrity, availability) that the system ought to support and these goals guide the procedures, standards and controls used in the design of the information security architecture. The policy must also define critical assets, perceived threats, and security-related roles and responsibilities.

Although each organization's security needs are unique, most security policies address common elements. Due to the dynamic nature of the ICT environment an information security policy is by no means set in stone, rather it is a living document. We recommend including the following elements in an information systems security policy (SANS, 2014):

a. **Objectives** - clearly states the reason the security policy exists.
b. **Scope** - identifies the people and systems affected by the policy.
c. **Protected Assets** - identifies the assets that the policy protects (e.g. e-mail servers, databases, and websites).
d. **Responsibilities** - identifies the groups or individuals responsible for implementing the conditions of the policy.
e. **Enforcement** - discusses the consequences of violating the policy.
f. **Remote Access Policy** - outlines acceptable methods for remotely connecting to the internal network (e.g. whether employees are allowed to connect to the network from their home computers).
g. **Information Protection Policy** - provides guidelines to users on the processing, storage, and transmission of sensitive information.
h. **Virus Protection Policy** - provides requirements for the use of antivirus software as well as guidelines for reporting and containing virus infections.
i. **Password Policy** - provides guidelines for how user-level and system-level passwords are managed and changed.
j. **Firewall Security Policy** - describes, in general, how firewalls are configured and maintained, and by whom.

Once the organisational information systems security policy has been developed the next step is

to establish the information security plan. While the policy defines the goals, the plan determines the steps that need to be taken to implement information systems security. Information systems security is not a separate task but an overlapping association of technologies, people, policies, and processes. The plan has to coordinate the whole effort to match the organisations' policy and ensure that there are no gaps (Microsoft, 2014).

We recommend the following four steps in developing an information systems security plan (Lichtenstein, 1997; WatchGuard, 2014 & Microsoft, 2014):

a) **Assess**: the current state of security, identify critical assets, predict threats and determine exposure for each asset.
b) **Plan**: for risks, noting that the objective is not to eliminate all risk regardless of cost but to minimise risks.
c) **Execute**: check for adequacy, obtain participant feedback, modify plan if required and implement the plan.
d) **Monitor**: research new threats as they become evident, modify the plan when changes occur (e.g. personnel changes) and perform ongoing maintenance (e.g. antivirus definition updates).

## CONCLUSION

Modern society is significantly dependent on IT and there is little likelihood that this will change in the future. As globalization continues to advance and electronic civil disobedience increases in volume and efficacy, the implementation of effective information security continues to become an area of concern for academics, information security researchers, information security practitioners and management of organisations (small and large). It is essential that all stakeholders are aware of security threats and trends and take appropriate steps to provide adequate protection of information system assets. Many researchers are of the opinion that what is good for large businesses is also applicable to small businesses. This view is based on the incorrect assumption (as noted in Lubbe, 2004) that research conducted in large businesses can be applied directly to small businesses.

Some concerns regarding SMEs are: 1) small businesses are trying to do everything by themselves (without enlisting expert assistance), and 2) small businesses are frequently exposed to crime, (especially technology related crimes). The rationale is that they (small businesses) do not have the base across which to spread the costs of hiring security experts or implementing expensive security-related technologies. Additionally, academic and non-academic studies in information systems security have concentrated primarily on large organisations. Possible reasons are that: 1) large businesses can make a greater contribution to the economy, and 2) that large businesses have bigger budgets and therefore can spend more on information security and security research.

With regard to small businesses, the findings reveal that this sector is rapidly growing and is making significant contributions to the economy. Furthermore, small businesses are embracing ICT and the Internet to gain competitive advantage, market share and access to new markets, solve business problems, and to accumulate knowledge for improvement of services. Innovative entrepreneurs are also using technology and the Internet as a means to market niche products and to reach distant customers. The above-mentioned reasons provide excellent justification for developing and building capacity regarding academic research into the information security crises facing small businesses.

There is no silver bullet to the information systems security problem in small businesses. Information systems security requires a firm grounding in academic theory in order to be effective. Security cannot be gained by installing a gadget, no matter how good it is. Security is a process that must be woven into the corporate culture of every organisation (small or large), with due attention to the ever-changing landscape of threats, vulnerabilities and risks. Any models or guidelines developed must be relevant and take cognisance of the fact that small businesses are unique and that they have their own focus and drivers when dealing with the information systems security problem. Information system security attacks and breaches make no distinction in the size of the organisation (small and large are equally at risk), the small business practitioner, however, has to recognise and manage information security risks without the resources available to larger businesses. It is therefore crucial that stakeholders are aware of security threats and trends and take appropriate steps to provide adequate protection of information system assets.

## REFERENCES


AusCERT (2006). *2006 Australian Computer Crime and Security Survey*.

Berger D.L., (1981). *Security for Small Businesses. Woburn, Mass: Butterworth Inc*.

Birman K.P., (2000). The next generation internet: unsafe at any speed. *IEEE Computer*. 33(8), 2000, pp54-60.

Blatchford C., (1998). Computer controls -- Diffusion into the smaller firm: (A Qualitative Research Study: Part 1), *Computer Fraud & Security*, Volume 1998, Issue 12, December 1998, pp13-17.

Campbell K., Gordon L.A., Loeb M.P., Zhou L., (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, 11(2003), IOS Press, pp431-448.

Business Continuity Management Survey [BCMS], (2003). Business Continuity Management Survey ZA 2003 [online]. KPMG. Available from: http://www.kpmg.co.za/download/BCSSURVEY_03.PDF. [Accessed 01/12/2014].

Cavusoglu H., (2002). The economics of information technology (IT) security. *2002–Eight Americas Conference on Information Systems*. Doctoral Consortium.

Cert (2013). *Cyber Crime and Security Survey Report 2013*.

Chelimsky E., Jordan F.C., Russell L.S. & Strack J.R., (1979). *Security and the Small Business Retailer*. Washington DC: Government Printing Office.

COBIT, (2014). COBIT 5: *A Business Framework for Governance and Management of Enterprise IT* [online]. Available from: http://www.isaca.org [Accessed 9/12/2014].

Computer Security Institute [CSI], (2011). *CSI/FBI 2010/2011 Computer Crime and Security Survey* [online]. Available from: http://www.gocsi.com/forms/fbi [Accessed 27/01/2005].

Deloitte (2013). *2013 TMT Global Security Study*.

Doney L.D., (1998). The Growing Threat of Computer Crime in Small Businesses, *Business Horizons*, vol.41 no.3, May-June 1998, pp81-87.

DTI, (2014). How to write an information security policy [online]. UK Department of Trade and Industry. Available from: http://www.dti.gov.uk/bestpractice/technology/security.htm [Accessed 18/03/2014].

EY (2014). *EY's Global Information Security Survey 2014.*

Farahmand F., Navathe S.B., Sharp G.P., Enslow P.H., (2003). Managing Vulnerabilities of Information System to Security Incidents. *Communications of the ACM*. 2003, pp348-354.

Galliers R., (1993). Research issues in information systems. *Journal of Information Technology*, 8(2): 92-98.

Garg A., Curtis J., Halper H., (2003). Quantifying The Financial Impact Of IT Security Breaches. *Information Management & Computer Security*, 11/2, 2003, MCB UP, pp74-83.

Glaser B.G. & Strauss A.L., (1967) *The Discovery of Grounded Theory*. Chicago, Aldine Inc.

Goodhue D.L. & Straub D.W., (1991). Security Concerns of System Users: A Study of Perceptions of the Adequacy of Security Measures. *Information & Management*. Volume 20, No. 1, January 1991, pp13-27.

Gordon L.A. & Loeb M.P., (2002). The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, Vol.5, No. 4, November 2002, pp438-457.

Gordon L.A. & Richardson R., (2004). Infosec Economics New Approaches to Improve Your Data Defenses. *Network Computing*, 4 January 2004, pp67-70.

IT Governance Institute [ITGI], (2001). *Information Security Governance*: *Guidance for Boards of Directors and Executive Management* [online]. Available from: http://www.isaca.org [Accessed 17/02/2005].

Jones, J (2014). *South Africa neglects alarming effect of cybercrime* [online]. Available from: http:// http://www.bdlive.co.za/business/2014/01/14/south-africa-neglects-alarming-effect-of-cybercrime [Accessed 9/12/2014].

Keogh J.E., (1981). *The Small Business Security Handbook*. Englewood Cliffs, New Jersey: Prentice-Hall.

KPMG (2012). *Luxembourg IT Security Survey 2012-2013*.

Lubbe S., (2004). *The use of IT in Small Businesses: Efficiency and effectiveness in South Africa.* (Paper submitted to SAJEMS for publication).

Lichtenstein S., (1997). Developing Internet Security Policy for Organizations. *Proceedings of the Thirtieth Annual Hawaii International Conference on System Sciences*. 1997. IEEE Computer Society.

Mehta M & George B., (2001). *Security in Today's E-World*. 2001-Eight Americas Conference on

Information Systems.

Mitchell R.C., Marcella R., Baxter G., (1999). Corporate information security management. *New Library World*, 1999 Volume: 100 Number: 5, pp213-227

National Small Business Act [NSBA], (1996). *National Small Business Act No. 102 0f 1996* [online].

South Africa Government Online. South African Parliament. Available from: http://www.info.gov.za/acts/1996 [Accessed 15/01/2005].

Norton (2013), *Norton Cybercrime Report* [online].Available from: http://www.norton.com/2012 cybercrimereport [Accessed 9/12/2014].

Ntsika Enterprise Promotion Agency [Ntsika], (2012). *State of Small Business Development in South Africa Annual Review 2012* [online]. Available from: http://www.ntsika.org.za/publications [Accessed 21/01/2014].

NZ (2010). *2010 New Zealand computer crime and security survey.*

Microsoft, (2014). *Security guide for Small Business* [online]. Available from http://www.microsoft.com/smallbusiness [Accessed: 18/03/2014].

Petkov D, Fry G.S., Petkova O. & D'Onofrio M., (2003). *Assisting Small Information Technology Companies Identify Critical Success Factors in Web Development Projects*. Ninth AMCIS.

Pipkin D., (2000). *Information security: protecting the global enterprise*. Prentice-Hall, 2000.

Posthumus S. & von Solms R., (2004). A framework for the governance of information security, *Computers & Security*, Volume 23, 2004, pp638-646.

Pratt J.H., (2002). *E-biz: Strategies for Small Business Success* [online]. Available from http://www.sba.gov/advo/research [Accessed 9/03/2005].

PwC (2014a). *2014 Information Security Breaches Survey*.

PwC (2014b). *BIS Cyber Security Breaches Survey 2014*.

PwC (2015). *The Global State of Information Security Survey 2015*.

Stoneburner G., Goguen A., & Feringa A., (2002). *Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology*. NIST Special Publication 800-30. July 2002. US Dept of Commerce.

Straub D.W. & Welke R., (1998). Coping With Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly.* December 1998, pp441-469.

Tsiakis T. & Stephanides G., (2005). The economic approach of information security. *Computers & Security*, Volume 24, Issue 2, March 2005, pp105-108.

US National Institute of Standards and Technology [NIST], (1995). *An Introduction to Computer Security: The NIST Handbook. Special Publication 800-12* [online]. US Department of Commerce. Available from: http://csrc.nist.gov/publications/nistpubs [Accessed 31/01/2005].

WatchGuard, (2014). A Practical Guide for Better Security [online]. Available from: http://www.watchguard.com [Accessed: 16/04/2014].

Vermeulen C. & von Solms R., (2002). The information security management toolbox – taking the pain out of security management. *Information Management and Computer Security*. Issue 10 Vol.3, 2002, MCP UP, pp119-125.

Von Solms B. & von Solms R., (2004). The 10 deadly sins of information security management, *Computers & Security*, Volume 23, Issue 5, July 2004, pp. 371-376.

Von Solms B., (2001). Corporate Governance and Information Security, *Computers & Security*, Volume 20, Issue 3, 1 May 2001, pp. 215-218.

Von Solms R., (1996). Information security management: The second generation. *Computers & Security*, Volume 15, Issue 4, 1996, pp281-288.