Investigating the Factors Inhibiting SMEs From Recognizing and Measuring Losses From Cyber Crime in South Africa

Gino Bougaardt and Michael Kyobe
University of Cape Town, South Africa
michael.kyobe@uct.ac.za

Abstract: The level of cyber attacks on organisations has increased tremendously in recent years. When such attacks occur, organisations need to assess the damage and loss from this crime. While large organisations have the mechanisms to determine such losses, SMEs lack such capability and often ignore the need to implement effective information security measures (Kyobe, 2008; Altbeker, 2000; Upfold and Sewry, 2005). Consequently, their risk exposure to cyber threats and the losses they incur from these attacks are often high (Ngo, Zhou, Chonka and Singh, 2009). However, the current legislative requirements, costly legal liabilities for non-compliance, and increasing pressure by stakeholders (e.g., lenders, business partners) on SMEs to comply with good practices suggest that SMEs cannot ignore security any longer. In order to ensure accountability and compliance with security requirements, it is imperative for SMEs to identify, account and report cyber incidents and losses resulting from cyber attacks. This study investigated the factors that inhibit SMEs from recognizing and measuring losses from cyber attacks in South Africa. A survey involving twenty organisations from different business sectors was conducted and the results indicate that victimisation, resulting from a lack of awareness of cyber-crime has the greatest influence on SMEs' ability to recognise and prepare losses from cyber attacks.

Keywords: cybercrime, recognition and measuring losses, SMEs, victimisation

1. Introduction

Despite the availability of numerous methods and publications on how organisations can manage information security risks, SMEs still face serious challenges in managing cybercrime and resulting losses. Cybercrime are criminal activities involving the use of electronic devices and may lead to incidents such as theft of information; Sabotage of data of networks; loss of information due to eavesdropping ; financial fraud; denied access to information; and damage due to virus attacks (Kshetri, 2009). These incidents result in financial and other losses to the organisations.

Many SMEs fail to identify or recognise and account for these losses. They fail to manage these risks and continue to ignore the implementation of effective information security measures (Kyobe, 2008; Altbeker, 2000; Upfold and Sewry, 2005). Consequently, their risk exposure to cyber attacks and the resulting losses continue to rise (Ngo, Zhou, Chonka and Singh, 2009). The current legislative environment, pressures from stakeholders (e.g., lenders, business partners) and liabilities in the event of violation of legal requirements make it imperative for SMEs to assess or estimate security risks and account for potential losses resulting from cyber attacks. Risk assessment is the process by which systems risks are identified and assessed in order to justify safeguards and protect systems from attacks (Carroll, 1996). Accounting for losses involves the evaluation and reporting of the damages when they occur. While studies on information security in SMEs are increasing, limited attention has been paid to SME inability to recognise and account for losses from cyber-crime.

The objective of this study is to identify the factors that inhibit SMEs from identifying/recognizing and measuring losses from cyber attacks. In addition, we also determine the degree of influence each of the identified factors has on SME ability to recognise and prepare losses. In the following sections, the authors review literature on factors inhibiting recognition and measurement of losses. A conceptual model representing the relationship between these factors is presented. The results of an empirical test of this model are then presented. This is followed by conclusions and recommendations for future research.

2. Literature review

The process of identifying, recognising and reporting losses from cyber crime has not been easy for many organisations. Numerous challenges have been identified. For instance, difficulties in understanding what cyber crime represents, difficulties relating to risk identification and analysis, weaknesses in data recording and interpretation, poor design of security systems, risk management and human behaviour (Canhoto, 2010). Some of these challenges are examined in more detail below:

Reference this paper as: Bougaardt, G and Kyobe, M. "Investigating the Factors Inhibiting SMEs From Recognizing and Measuring Losses From Cyber Crime in South Africa" *The Electronic Journal Information Systems Evaluation* Volume 14 Issue 2 2011, (pp167-178), available online at www.ejise.com

2.1 Lack of awareness of cybercrime and lack of knowledge of being a cybercrime victim

In his position paper to the Oxford Internet Institute, Baker (2010) argues that the process of collection and analysis of cybercrime data is often affected by a lack of understanding of what cybercrime means or represents. This lack of understanding of cybercrime, which is also evidenced by various ambiguous and conflicting interpretations of the term, impedes its recognition and measurement. Many organisations continue to be victimised because they are not aware of the nature or characteristics of this crime. Theories of victimisation explain the persistent victimisation of individuals and organisations by cyber criminals. Gottfredson and Hirsch (1990) in their General theory of crime, and Shreck et al (2003), in their work on victimisation show that victimisation results from low levels of self-control. A lack of self-control (defined here as the inability to control oneself or one's emotions), is reflected in behaviours like short-sightedness, being insensitive or being impatient. SME managers are reported to be insensitive to cybercrime (Jacque, 2003; Zorz, 2003). Individuals with low self-control are believed to make decisions exclusive of those situations that increase their vulnerability and fail to change or mitigate their risk factors after the first victimisation (Forde and Kennedy (1997). This also renders several victimisation surveys inaccurate as they often underestimate incidence and prevalence rates (Fafinski, 2010).

Solms and Solms (2004) assert that the lack of awareness sin is still committed by many companies. There are no proper awareness training programs and consequently, users are unaware of the risks of using their IT infrastructure and the potential damage they can cause to it.

2.2 Lack of risk management skills

The goal of risk management is to identify, measure, control and minimize losses associated with uncertain events (Patel and Zaveri, 2010). SMEs fail to recognise and measure losses because they do not engage in record keeping and IT risk assessment and management (Dimopoulos, Furnell and Barlow, 2003). Dimopoulous et al. (2003) attributes this to the lack of funds, expertise and awareness of security risks. Risk analysis is perceived by SMEs as being complex, requiring specialist expertise and therefore something to be outsourced (Dimopouloulous et al (2003). It is also thought to disrupt management and employee activities throughout its duration. Furthermore, existing models (e.g. CRAMM) for evaluating the benefits of reducing the risks versus the investment in security technology are difficult to understand or use by SMEs (Dimopoulous et al., 2003). There are also challenges involved in comprehending the results and reports generated by these tools. The identification of risks is made harder for smaller organisations due to changes in technology and modes of vulnerabilities (Srinivasan and Abi-raad, 2003).

2.3 Information system security design/infrastructure

The design of the security system may also impact on the recognition and estimation of losses. Modern business environment comprises of many different applications and systems and each of these has its own threat profile (Conklin and Dietrich,2008). Such environment creates challenges for security practitioners responsible for developing security solutions. Consequently, these developers are forced to come up with piecemeal security designs, often disjointed, patched and can not monitor and comprehensively report on the security environment in the organisations (Conklin and Dietrich, 2008).

Acccording to Canhoto (2010:1), the technical characteristics of the environment also influence how data on losses is derived and expressed e.g., data format, content and threshold, and which alerts and reports are produced. He states further that "formal aspects of the environment such as policies or regulations provide general definition of cybercrime, and may specify signs of alarm and the expected behaviour from analysts that detect such signs". SMEs usually do not possess security and compliance policies (Kyobe, 2008), and as indicated above, many do not engage in formal planning. Therefore such signs of alarm are often not identified before hand.

2.4 Management attitude to security

Individual cognitive processes, e.g., expectations, stereotypes and prior experiences, may influence attitude to security and the nature of data identified (Canhoto, 2010). Researchers argue that the failure by entrepreneurs and small business managers to proactively implement measures to handle

risks has more to do with their personal characteristics (Ndubusi et al., 2005; Sjöberg et al., 2004; Nattaradol, 2002; Orford et al., 2004). Proactive-risk handling is defined as the process in which potential risks to a business are identified in advance, analyzed, mitigated and prevented, and the cost of protection balanced with the cost of exposure to the risk. This does not appear to be done by small business managers or entrepreneurs. For instance, many entrepreneurs in South Africa are reported to have started businesses without giving proper consideration to economic, environmental, and cognitive limitations (Orford et al., 2004; Ladzani and Netswera, 2003). In his report on ICT adoption by rural SMEs in Thailand, Nattaradol (2002) also shows that lack of proactiveness and proper evaluation of ICT projects resulted in misjudgment or under-estimation of potential business and security risks. He identified several practices in ICT adoption which are indicative of irrational planning or behaviors (e.g., failure to estimate project costs, use of unskilled or untrained staff to manage ICT installations, use of obsolete hardware and software and ignoring potential impact of hackers and sneakers).

In addition, small business managers tend to have a strong desire for autonomy and control which could easily hamper the success of the organization (Kyobe, 2006). They tend to be rigid, traditional and usually do not draw up definitive duties or responsibilities for their subordinates. The high degree of generality resulting from undertaking heterogeneous work prevent employees from developing expertise in dealing with IT security issues (Kyobe, 2006).

It is also widely reported that because of their false sense of security, small business managers are complacent about cyber-attacks and often shun good security systems and practices (Zorz, 2003;Jacque, 2003). Jensen (2004) found that security only became of much greater concern for the entrepreneurs once they had adopted e-commerce and experienced the reality of risks. Freeman (1999) explains this behaviour using Kübler-Ross' (1969) loss model. He argues that organisations response to major environmental change is similar to individual response to loss. According to Kübler-Ross' (1969) stage theory of loss, many who suffer loss proceed through these five stages – denial, anger, bargaining, depression, and acceptance. At the first stage, the person denies that the loss is inevitable. Freeman argues that this happens to organisations as well. Citing the work of Starbuck, Greve & Hedburg (1978), Freeman shows that managers would deny the extent of organisational crises to avoid blame.

Another problem related to this is the unwillingness by managers to report cyber attack incidents. In many cases the victims withhold reporting (Lee, 1997). The importance of reporting incidents has been emphasised in many studies on information security and safety. Today, organisations are required to implement information security reporting schemes based on standards like BS-7799/ISO-17799 (ISO-IEC 27002 (ISO, 2007) (Calder and Watkins, 2005). Gonzalez (2005) maintains that information security reporting is a quality improvement process that is essential to reduce incidents and Sveen et al (2007) state that to learn from an incident and avoid it in the future the incident's causes must be investigated by competent people. They caution however that the quality of an investigation is a function of the resources available and the workload. If for instance, resources are fewer than the allocated workload, this quality may be compromised. Phimister et al (2003) add that sporadic emphasis and management fear of liability may also hinder success in an incident reporting system. Eurim (2003) outlines several barriers to reporting including concern about confidentiality, disruption to business and loss of reputation. A culture of reporting does not exist in many SMEs due similar reasons outlined above (Kyobe, 2004;2006).

2.5 Lack of knowledge of, and compliance with security regulations

Cybercrime regulations require that organisations and individual recognise and account for damages resulting from cybercrime. Therefore a lack of knowledge of these security regulations and compliance with their requirements suggest inability to recognise and report on cyber-crime risks and losses. In South Africa cybercrime is regulated by the cyber crime section in Chapter XIII of the ECT Act, 2002 (Michalson, 2005). This chapter introduces statutory criminal offenses relating to unauthorized access to data (e.g., through hacking), interception of data (e.g., tapping into data flows or denial of service attacks), interference with data (e.g., viruses) and computer related extortions, fraud and forgery. They also state that a person aiding those involved in these crimes will be guilty as an accessory. A person convicted of an offence related to the above is liable to a fine or imprisonment for a period not exceeding five years.

Kyobe (2008) found that majority of the SMEs surveyed were not proactive in their approaches to compliance with such regulations. Few firms planned their security systems, allocated sufficient resources for compliance, trained their staff regularly and developed policies. Economical factors such as indirect compliance costs were found to be the main barriers to SME compliance in this study. Kyobe (2008) found that of the 30 South African Websites investigated, 40 percent had not implemented necessary legal requirements. 54% of all respondents never reported their effort towards compliance to auditors and 32 percent of the respondents were not aware of the requirements and liabilities of the ECT Act.

2.6 Summary

The key relationships as described in the previous sections are presented in the conceptual model in Figure 1 below. This model was then validated empirically in a study involving 20 SMEs as indicated in the following sections.

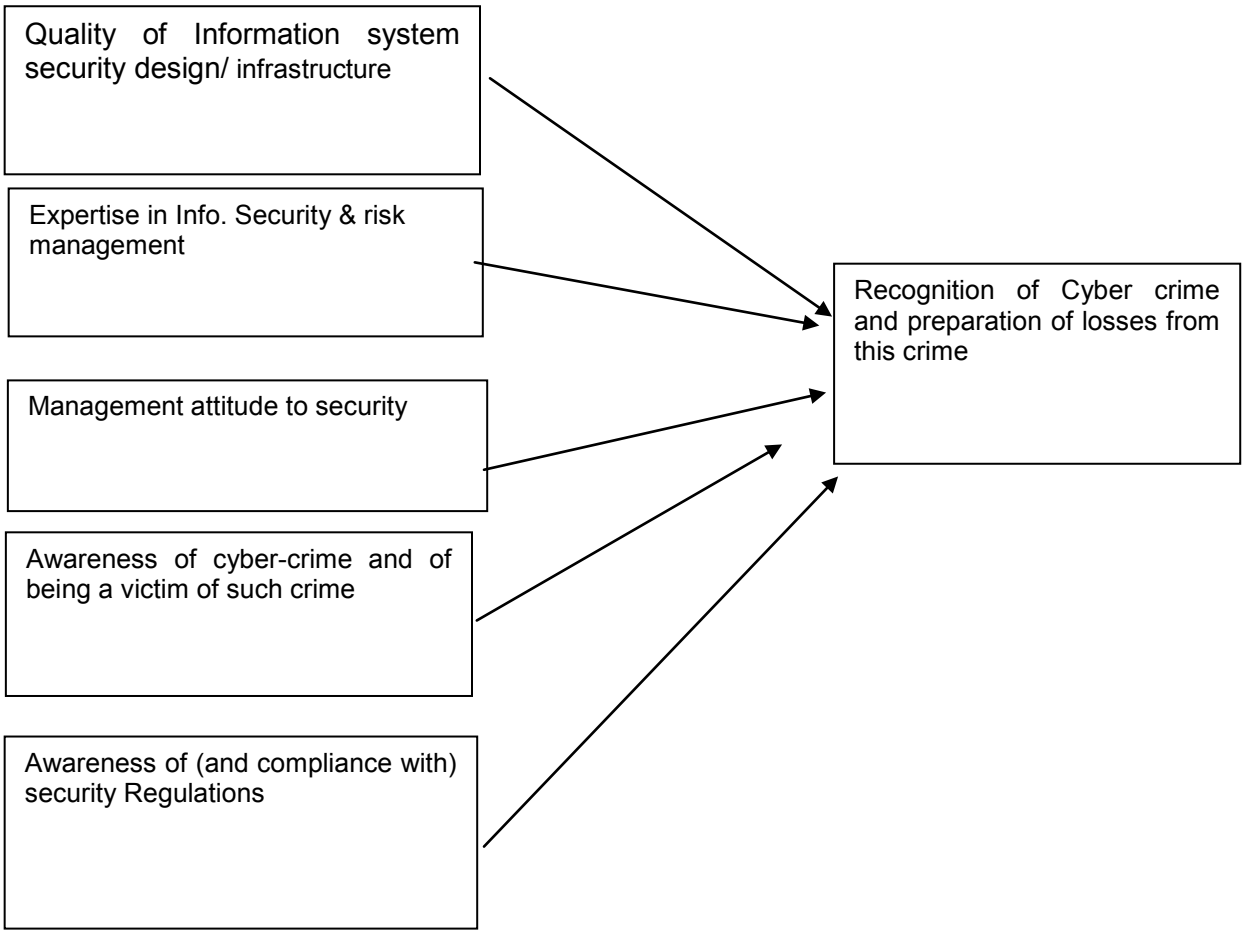

Figure 1: Conceptual model

3. Methodology

Senior management and employees responsible for IT/IS infrastructure in SMEs were targeted since they mainly make decisions relating to IT. The respondents were requested to identify their positions in the SME. An up-to-date database from the South African SME Toolkit web site (http://southafrica.smetoolkit.org) was initially used to identify SMEs engaged in e-commerce. This database consists of current information and was not for purchase. There are other alternative SME databases like Braby business directory. However, these are available at a fee which was not affordable in this project.

The content administrator of the SME Toolkit web site first confirmed via email that the majority of the businesses registered on the web site are SMEs and their details are updated annually. The content administrator noted that it is their policy to remove the profiles of the SMEs from their web site if the

SMEs do not update their details annually. Using the above database and focusing on South Africa only, the researchers compiled an excel spreadsheet containing the following information about the SME: industry (and sub-industries); business name; and email contact details (SME ToolKit, 2010). The excel spreadsheet contained 420 SME details. 26 duplicate entries were removed. Some of the duplicates existed because some firms were registered in more than one industry and sub-industries. 394 entries were left on the database. Each of these entries was then given a unique number and 300 SMEs were then selected for this study. This was done using simple random sampling method. Excel's random number generator function was used to randomly identify these 300 SMEs.

4. Data collection

A questionnaire was used to reach the many people in our sample. The constructs and their measures were mainly adapted from previous research papers (Kyobe,2008; Upfold and Sewry, 2005; and Herath and Rao, 2009), see Table 1 below.

Table 1: Constructs and measures

Construct	Measure	Questions Adapted from
Quality of Information Security Design/Infrastructure	-Our information security solution protects the entire business system -Use up-to-date software and Hardware -Use anti-virus software -Use a firewall and data encryption	Kyobe (2008)
Lack of expertise in (Information security & risk management)	-Availability of IS/IT expertise in security -Seek expert assistance from external sources -Techniques employed are useful in determining cyber losses -experience difficulties using estimation techniques	Upfold and Sewry (2005)
Management attitude to security	-Mitigate threats or risks to business/IT systems -Discipline employees who violate security regulations - Train staff on IS risks - false sense of security - readness/willingness to report incidents	Kyobe(2006, 2008)
Lack of awareness of cyber-crime and of being a victim of such attacks	-Our system is often unavailable due to cyber attacks -Have suffered financial loss due to cyber attacks -	Kyobe(2008)
Awareness and compliance with regulations	- have documented a Security policy -Comply with the ECT Act -employees are aware of the ECT Act requirements and penalties	Kyobe(2008)
Recognise computer crime and prepare losses	- Perform record keeping -availability of expertise in preparing loss estimates - prepare financial loss estimates due to computer attacks -possess expertise in preparing financial losses we document information security activities - we conduct information security audits	Upfold and Sewry, 2005; and Herath and Rao, 2009

The first part of the questionnaire obtained general information about the respondents. Subsequent sections measured the different aspects of the research model i.e., quality of the security infrastructure, expertise in information security management, the attitudes of management towards information security, awareness of cyber-crime and acknowledgement of being a victim of such crime, knowledge of the security regulation and the extent to which SMEs recognise cyber crime and prepare losses.

The questionnaire was piloted with one academic and was approved by the University Ethics Committee. It was then attached to an email consisting of a cover letter and sent to the SMEs. On average about 30 SMEs were grouped per email so as to avoid congestion on the University's network. The researchers used the University email account to launch this research project since it offered greater credibility to the research project as opposed to non-University email accounts. The SMEs were all blind-copied in the email to ensure confidentiality.

The initial responses were disappointing, only 11 responses were received. Follow up emails were sent to SMEs encouraging those who had not responded to do so (Saunders, et al., 2009, p. 397-398). However, we never received any more responses. We therefore decided to increase the response rate by sending out 153 additional questionnaires. The additional SMEs were obtained from the following sources and were selected at random: The Waverely Business Park, Business Broadcaster, Facebook, Former colleagues and UCT Postgraduate students (Business Broadcaster, 2010; The Waverley Business Park, 2010). 11 addition responses were received making the total responses 22. In total, 453 emails were sent out. However, 163 bounced back. We can assume therefore that 290 emails were received although we have no way of confirming this. The response rate was therefore approximately 8%. Several factors might have contributed to the poor rate. For instance, by sending out an average of 30 emails, it is likely that such stream of emails would be directed to junk mail or deleted. It is also known generally that SMEs do not usually respond to questionnaires. Earlier studies suggest an average response rate of between 25-30% (Kyobe, 2008).

5. Results

Table 2 indicates the demographics of the respondents. It shows that 9 of the organisations are from the ICT business sectors. There are 11 organisations based in the Western Cape and 6 organisations based in Gauteng. Further analysis revealed that 5 of the respondents were IT/IS staff while the rest were business owners/managers). Furthermore, business managers had between 2 to 11 years experience trading on the Internet and 9 to 27 years of computer experience. IT/IS manager had 0 to 5 years of trading on the internet and 4 – 15 years of computer experience.

Table 2: SME demographics

	No. of Employees	Business Sector	Location	Yrs trading on Internet	Respondent Position	Respondent yrs of computer experience
1	4	Engineering Consulting	Western Cape	5	Owner	5
2	30	Information Technology	Western Cape	0	Consultant (IT)	15
3	12	NGO	National	0	Software Developer (IT)	10
4	150	Broadband provider-ICT	Western Cape	11	BP Manager-	9
5	9	Procurement to Mining & Industry	Gauteng	4	Manager	10
6	1	Information Technology	Western Cape	1	Owner	20
7	6	Telecoms	North West	10	Sales Director	18
8	2	Accounting	Western Cape	4	Director	11
9	24	Construction	Limpopo/KZN/Mpumalanga		Director	10
10	2	IT	GT	5	Director	15
11	15	IT Consulting	Gauteng	3	CEO	17
12	1	ICT	Gauteng	1	CEO/Project Manager (IT)	4

	No. of Employees	Business Sector	Location	Yrs trading on Internet	Respondent Position	Respondent yrs of computer experience
13	5	Management Consulting	Gauteng	2	Managing Director	10
14	1	Consultancy	Western Cape	2	Owner	27
15	7	Information Technology	KZN	2	MD	20
16	8	Financial Services	Western Cape	11	Director	20
17	46	Building	Western Cape	6	CEO	12
18	1	Financial Services	Western Cape	10	Senior Architect/ Strategist	16
19	80	Market Research	Western Province	0	IT Development Team Leader	10
20	80	Online Gaming	Western Cape	5	Architect (IT)	5
21	47	Construction	Western Cape	9	Marketing Director	11
22	20	Insurance	Gauteng	3	Director	25

6. Reliability assessment

The reliability test was conducted using the Cronbach's alpha (Saunders, et al., 2009, p. 374). The Cronbach alpha coefficient above the recommended 0.70 would confirm the reliability of the questions used (Nunnally, 1978). Table 3 shows the reliability test results for the constructs in the conceptual model.

Table 3: Assessment of reliability

Constructs	No.of Items	Cronbach Alpha
Quality of IS Security Design	3	0.70
Lack of Expertise: Info. Security	4	0.82
Management attitude to security	4	0.73
Awareness of cybercrime (victimisation)	4	0.88
Awareness of (and compliance with)security regulations	3	0.75
Recognise computer crime & prepare losses from cyber crime	5	0.82

The Cronbach alpha coefficients (in Table 3) are above the recommended 0.70 (Numally, 1978), thereby confirming reliability or internal consistency of the variables used in the present study. Most variables as stated above were adapted from prior studies. This also assisted in ensuring construct and content validity.

7. Analysis

Table 4: Mean responses

	No. of Items	All respondents		Business Managers		IT/IS staff	
Constructs		Mean	Std	Mean	Std	Mean	Std
	No. of Items	All respondents		Business Managers		IT/IS staff	

Quality of IS Security Design	3	3.41	1.13	2.99	0.65	3.77	0.77
Lack of Expertise: Info. Security	4	2.99	0.99	3.50	1.00	3.50	0.99
Management attitude to security	4	2.49	0.91	2.19	0.65	3.90	0.97
Awareness of cybercrime (victimisation)	4	3.01	1.16	2.27	0.88	3.98	0.88
Awareness/compliance with security regulations	3	2.45	0.73	2.59.	0.66	3.31	1.12
Recognise & prepare losses from cyber crime	5	2.47	0.37	2.84	0.60	3.67	0.76

7.1 Correlation analysis

Correlation analysis was conducted to determine the association between variables.

Table 5: Correlation analysis

	1	2	3	4	5	6
1. Quality of IS security design	1					
2. Lack of expertise in IS	**0.21**	1				
3. Management attitude to security	**0.39**	0.44	1			
4. Awareness of cyber crime attacks (victimisation)	**0.11**	**0.22**	0.35	1		
5. Awareness/compliance with regulations	0.**31**	**0.33**	0.07	0.48	1	
6. Recognise & prepare losses from cyber crime	**0.18**	**0.28**	**0.21**	**0.37**	**0.19**	1

* (correlations significant at .05 or less are shown in bold)

8. Discussion of findings

Table 4 shows that most respondents were not certain about the quality of IS security design (mean score was 3.41). They were not certain if their systems (i.e., Firewall, software, hardware and anti-virus software) really protected their businesses. Further analysis reveals however that many respondents were using up-to-date hardware and software. For instance, of the 17 business managers, 14 used up-to-date software and hardware; 13 used anti-virus software and 14 used a firewall and encrypted data. This suggests therefore that SMEs possess up-to-date technologies but do not utilise them effectively to provide accurate and reliable security information. Most anti-virus software would provide reports on the frequency and nature of attacks which is useful in determining the extent of the damage. There was a positive and significant association between information security design/infrastructure and the dependent variable (see Table 5, item 6 - recognise and prepare losses from cyber crime).

Further evidence of inability to compile reliable information necessary for determining losses from cyber attacks is revealed by the lack of expertise in information security. While the mean result for this item is closer to uncertain (2.99), further analysis indicates that most respondents agreed to some extent that such skills were lacking. Of the 17 business managers, only 3 seek external expertise on information security; only 3 had used the techniques for determining financial loss estimates from cyber-attacks successfully and another three indicated that they had experienced difficulties in using estimation techniques. Most of the other business respondents were uncertain about all this which suggests difficulties or inability to compile information about cyber-attacks. Table 2 indicates that ½ of the respondents had more than 10 years of IS/IT experience. However, since many could not identify and determine the losses, this suggests that possession of IT skills does not necessarily translate into proper management of IS security risks. Table 5 shows a positive and significant association between quality of information security design and the dependent variable. This suggests therefore that the

former does influence the latter. Insufficient knowledge or awareness of IT risks and computing limitations are major factors inhibiting small organizations from engaging in effective planning and monitoring of business operations (Kyobe, 2004).

Table 4 also shows that overall most respondents seem to ignore information security requirements. The mean score was 2.49 indicating rather a negative attitude or lack of attention to security requirements. Management attitude to security was measured by asking respondents to indicate whether they mitigated risks, disciplined employees who violated security requirements, trained staff on IS risks and reported security violations. Further analysis of the responses of business managers and those in IT/IS staff confirms that information security is not a major concern for business managers (mean score for business managers was 2.19 compared to 3.90 by IT/IS staff). It is not surprising therefore that Table 5 reveals a significant correlation between Management attitude to security and (quality of IS security design and lack of expertise in IS security). These influence SME ability to recognise losses as confirmed by the positive and significant relationship revealed in Table 5.

In the case of awareness of cybercrime (and victimisation), the overall mean response was 3.01 (see Table 4), which suggests the respondents were uncertain. However, a breakdown of the responses indicates that only those with technical skills appear to be aware that their systems were unavailable due to cyber attacks and that they do suffer losses due to cyber attacks (mean score was 3.98). Business managers were mainly uncertain of the potential for victimisation. Further analysis shows that of all the 17 business managers that participated in this study, only 3 were aware that their systems were unavailable due to computer attacks and only 4 indicated that they had suffered financial losses due to computer attacks. Further, the results of Compliance with security regulations also appear to confirm the problem of lack of awareness of cyber risks. The mean score was 2.45 (disagree). This may not be surprising given the fact that most business managers were also found to be least concerned about information security risks and also did not know they were potential victims of cyber attacks. With limited understanding of the nature of cyber-attacks, there is also bound to be several different interpretations of these attacks which make it difficult to measure the losses. Lack of awareness of the requirements can also be contributed by failure to communicate information about these requirements and also inability to disseminate knowledge about those incidents. Such knowledge can be gained by studying security or incident reports, audit reports, and financial losses from attacks.

The analysis of compliance results show that even IT/IS staff were not certain whether they complied with security regulations (mean score was 3.31). 8 (out of 17 business managers) had documented an information security policy; 4 (out of 17) comply with the ECT Act requirements and only 3 (out of 17) indicated that their employees are aware of the ECT Act requirements and penalties. This confirms Jacque's (2003) observation that SME managers were insensitive to cybercrime. Such level of insensitivity translates into lack of self control which results into re-victimisation (Shreck, 2003). The fact that this construct was found to be associated with recognition and reporting of losses from cyber-attacks confirms that lack of compliance influence SME ability to prepare losses.

Table 4 also shows most respondents did not agree that they recognise and prepare losses from cyber attacks (Mean score 2.47). However, some IT/IS staff indicated they do so to some extent (3.67). Recognition and preparation of losses from cyber attacks was measured by asking respondents to indicate if they kept records, possessed expertise in preparing losses, document information security incidents and conduct security audits (see Table 1). Further analysis shows that of the 17 business managers, only 2 prepared financial loss estimates due to cyber-attacks; 5 perform record keeping and auditing; 7 document information security activities and 7 conduct information security audits. While a number of organisations indicated that they recognise and prepare accounts of losses, the results obtained from the compliance construct suggest that the findings of these reports are not disseminated for the benefit of others. Table 5 shows that all other constructs were significantly correlated with this construct.

8.1 Regression analysis

We also conducted a regression analysis to determine the relationships between the variables. The results in Table 6 suggest that in the South African SMEs, lack of awareness or victimisation has the most influence on SMEs' ability to recognise and measure losses from cyber crime than lack of expertise in information security management and management attitude to security. It is surprising to

find in this study that quality of IS design and awareness and compliance with regulations did not have significant influence on recognition and measuring losses. This could be attributed to the small sample size and the number of items used to measure these constructs. It is however interesting to find that our suspicion regarding three of the constructs (i.e., lack of awareness of cyber-crime (victimisation); management attitude to security; and lack of expertise in risk management) were found to be correct in this analysis

Table 6: Regression summary for dependent variable: Recognising & measuring losses from cyber crime

R = 0.8209 ; R Sq = 0.6739; Adjusted R Sq = 0.5720; F(5,16) =6.6132; p < 0.00162; Std.Error of estimate: 0.68841						
	Beta	**Std Err of Beta**	**B**	**Std Err of B**	**T(16)**	**P=level**
Intercept			2.5642	1.8677	1.8436	0.01887
Quality of IS design	-0.1238	0.1611	-0.2151	0.2798	-0.7678	0.45232
Lack of expertise	0.3394	0.1895	0.35110	0.1959	1.7914	0.04932
Management attitude to security	0.4621	0.2177	0.1299	0.0612	1.1234	0.04365
Lack of awareness (victimisation)	0.8119	0.2034	1.11080	0.2783	3.990	0.00105
Awareness & compliance with regulations	0.5262	0.2431	1.0391	0.4800	2.1648	0.4589

9. Conclusion

This study shed more light on those factors influencing recognition and measurement of losses from cyber attacks in SMEs. Three major problems are identified: First, lack of awareness and understanding of what cyber-attacks involve, resulting in the continued victimisation of these firms. Lack of awareness makes identification, measurement and interpretation of data relating to cyber attacks difficult and as such losses may be difficult to determine (Baker, 2010). There is therefore great need for SME management to engage in IT risk management practices (Sanchez, Ruiz, Fernandez-Medina, and Piattini, 2010) although this may also require a change in attitude or in the way information security is perceived by SME managers (Upfold and Sewry, 2005; Kyobe, 2008).

In addition, there appears to be limited effort to ensure accurate and reliable data for the purpose of analysis even in those organisations that claimed to have up-to-date software, hardware and anti-virus programs. Latest anti-virus programs provide detailed reports on the frequency and nature of attacks which could be useful in the assessment of damages and losses. Without accurate and reliable measurements of events, it makes it difficult to report on losses (Baker, 2010).

We also found that while some organisations claim to recognise and prepare loss estimates, their employees are still unaware of the requirements of the ECT Act and penalties. This is probably caused by lack of dissemination of the findings, audit reports and incident reports to the stakeholders. Previous research shows the difficulties involved in releasing such information. Many organisations are reluctant to share such information due to fear of potential loss of reputation, confidentiality, and disruptions to business activities by law enforcement agencies. However, without sharing such information, awareness will not be created and the seriousness and risks involved in using IT systems would not be understood.

Several recommendations are provided on how SMEs can address this problem. Creating awareness through training on cyber-attacks, training in record-keeping practices and use of readily available statistics on crime, attacks and vulnerabilities, which is available online. Organisations should leverage the resources provided on the Internet, e.g., services that scan open-source material for potential damage and virus alert services. All these assist in creating awareness and in providing the much needed statistics about the losses. It is also useful to understand how to use most of the available software. For instance, Windows operating system provides firewall facilities and reports; anti-virus programs also provide audit reports based on actual results which is useful in providing reliable data to determine the losses. It is also important for organisations and government to provide SMEs with some incentives for reporting incidents since many are reluctant to disclose incidents or losses. We also believe the confusion surrounding measurement of cyber-attack losses relate to the

many regulations they have to comply with. Unless these are clearly understood, and what to report is known, organisations with limited legal, accounting and technical skills would find it difficult to get involved. Recognition and reporting of losses is therefore influenced by several factors and this implicates a combined strategy that encourages awareness, training, ability to measure reliable information and sharing it with other affected parties in an effort to devise common strategies

The findings presented in this paper are however based on evidence gathered from only twenty two SMEs. This is a major limitation therefore precautions need to be taken when generalizing these findings. This study should be repeated with a much larger sample and the relationships between the constructs tested again in a regression analysis. Given the limited sample size, we could not compare the responses of business managers and IT/IS staff. This could reveal more details about the potential causes of different behaviors of managers towards security. Future studies should investigate these relationships and their impact on the dependent variable.

References

Altbeker, A. (2000). *E-security: The race against computer crime.* Retrieved March 06, 2010, from http://www.iss.org.za/PUBS/CRIMEINDEX/00VOL4NO6/ESecurity.html

Baker, W.H. (2010). Thoughts on Mapping and Measuring Cybercrime. Oxford Internet Institute Forum Mapping and Measuring Cybercrime. http://www.sfu.ca/~icrc/content/oxford.forum.cybercrime.pdf. Page 26.

Calder, A., and Watkins, S., (2005), IT Governance, 3rd edition, Kogan Page, London

Canhoto, A. (2010). What' before 'How'. Oxford Internet Institute Forum . http://www.sfu.ca/~icrc/content/oxford.forum.cybercrime.pdf.

Carroll, J. M. (1996). Computer Security. Third Edition, Newton: Butterworth- Heinemann

Conklin, W. A., and Dietrich, G. (2008, January 7). Systems Theory Model for Information Security. *Proceedings of the 41st Hawaii International Conference on System Sciences - 2008*, (pp. 1-9). Big Island, Hawaii.

Dimopoulos, V., Furnell, s.m., and Barlow, I.M. (2003).Considering IT Risk Analysis in Small and Medium Enterprises. Proceedings of the 1st Australian Information Security Management Conference 2003 (InfoSec03), Perth, Australia, 24 November 2003

Available: scissec.scis.ecu.edu.au/proceedings/2003/infosec/pdf/02_final.pdf

EURIM (2003) IPPR E-Crime Study Partnership Policing for the Information Society. Working Paper 1: Reporting Methods and Structures. http://www.eurim.org/consult/e-crime/dec03/ECS_WP1_web_031209.pdf

Fafinski, S. (2010) Mapping and Measuring Cybercrime, Position Paper. p75. Mapping and Measuring Cybercrime. http://www.sfu.ca/~icrc/content/oxford.forum.cybercrime.pdf. Page 36

Forde, D., and Kennedy, L. (1997). Risky lifestyles, routine activities, and the general

theory of crime. *Justice Quarterly,* 14, 265-289.

Freeman, S. (1999). Identity Maintenance and Adaptation: A Multilevel Analysis of Response to Loss. *Research in Organizational Behavior, 21*, 247-294.

Gonzalez, J.J. (2005), *Towards a Cyber Security Reporting System – A Quality Improvement Process*, Springer, Berlin Heidelberg

Gottfredson, Michael R., and Travis Hirschi. 1990. *A General Theory of Crime*. Stanford, CA: Stanford

University Press.

Herath, T., and Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems , 47* (2), 154-165.

Jaques, R. (2003). Survey finds firewall and antivirus software considered unimportant by SMEs, URL (Consulted September, 2004): http://www.frame4.com/php/printout689.html

Kyobe, M. (2006). *Entrepreneur behaviors on e-commerce security*, In M. Khosrow-Pour (ed.) Encyclopedia of e-commerce, e-government, and mobile commerce**,** pp. 437-444).

Kyobe, M. (2008). *Evaluating Information Security within SMEs engaged in E-commerce in South Africa.* Retrieved March 08, 2010, from http://www.isbe.org.uk/Kyobe

Ladzani, M.W., and Netswera, F.G. (2003). Lessons from successful South African rural entrepreneurs, URL (Consulted October, 2007): http://www.sbaer.uca.edu/research/icsb/2003/papers/48.doc

Lee, W. (1997). A Deterrent Measure Against Computer Crime:

Knowledge-Based Risk-Analytic Audit, *Singapore Management Review,*

January, pp 19-45.

Michalson, (2009). " Protection of Personal Information Bill - the implications for you". Michalson.com. [Online] Available: http://www.michalsons.com/protection-of-personal-information-bill-the-implications-for-you/3041. Access date: 10 January 2010

Nattaradol, P. (2002), Harnessing ICT potential for the benefits of farmers and the rural poor: Experience and vision of Bank for agricultural cooperatives (BAAC), Thailand. BAAC. URL (Consulted October, 2007): http://www.adb.org/annualmeeting/2002/seminars/presentation/nattaradol_presentation.pdf.

Ndubisi, N.O., Gupta, O.K., and Ndubisi G.C. (2005). The Moguls' Model of Computing: Integrating the Moderating Impact of Users' Persona into The Technology Acceptance Model, *Journal of Global Information Technology Management*, 8(1): 27-47.

Ngo, L., Zhou, W., Chonka, A., and Singh, J. (2009). Assessing the Level of I.T. Security Culture Improvement: Results from Three Australian SMEs. *IECON '09 35th Annual Conference of IEEE 2009*, (pp. 3189-3195). Porto, Portugal.

Nunnally, J. C. (1978). *Psychometric Theory.* New York: McGraw-Hill.

Orford, J., Herrington, M., and Wood, E. (2004). *South African Report Global Entrepreneurship Monitor*. Retrieved January 22, 2005, from www.gsb.uct.ac.za/gsbwebb/userfiles/GEM_ 2004.pdf .

Patel, S. and Zaveri, J. (2010). Assessment model of cyber-attacks on information systems. Journal of computers, 15(3): 352-359.

Phimister,J., Oktem,U., Kleindorfer,P.R, and Kunreuther, H. (2003). Near-Miss Incident Management in the Chemical Process Industry. Risk Analysis, Volume 23, Issue 3, pages 445–459, June 2003

Sanchez, C.R, Fernández-Medina,E., and Piattini, M. (2010): Managing the Asset Risk of SMEs. ARES 2010: 422-429

Saunders, M., Lewis, P., and Thornhill, A. (2009). *Research methods for business students* (5th ed.). Harlow: Pearson Education Limited.

Schreck, C.J., and Miller, J.M. (2003). Sources of fear of crime at school: What is the relative contribution of disorder, individual characteristics, and school security?, *Journal of School Violence* **2** (2003), pp. 57–77.

Solms, B, and Solmns R. (2004). The 10 deadly sins of information security management, *Computer & Security* 23(5): 371-376.

Sjöberg, L., Moen,B., and Rundmo, T. (2004). Rotunde Publications 84. Explaining risk perception. An evaluation of the psychometric paradigm in risk perception research, URL (Consulted February, 2005): http://www.svt.ntnu.no/psy/Torbjorn.Rundmo/psychometric_paradigm.pdf

Srinivasan, G., and Abi-raad, M. (2003). Risk factors associated with e-buziness infrastructure of SMEs. Paper 21. 1st Australian Information Security Management Conference, Perth, W.Australia.

Sveen, F., Rich, E., and Jager, M. (2007), "Overcoming organizational challenges to secure knowledge management", *Information Systems Frontiers*, Vol. 9 No.5, pp.481.

Upfold, C. T., and Sewry, D. A. (2005). *An Investigation Of Information Security In Small And Medium Enterprises (SME's) In The Eastern Cape.* Retrieved March 06, 2010, from http://icsa.cs.up.ac.za/issa/2005/Proceedings/Research/082_Article.pdf

Zorz, J.(2003, May 15). Small firms 'shun' PC security. BBC NEWS. Retrieved October 15, 2004, from http://www.net_security.org/news:php?id=2650.

