ADOPTION OF INFORMATION TECHNOLOGY SECURITY POLICIES: CASE STUDY OF KENYAN SMALL AND MEDIUM ENTERPRISES (SMES)

[1]MICHAEL KIMWELE, [2]WAWERU MWANGI, [3]STEPHEN KIMANI

[1]Institute of Computer Science and Information Technology
Jomo Kenyatta University of Agriculture and Technology,
P. O. Box 62000- 00200 Nairobi, Kenya

[2]Institute of Computer Science and Information Technology
Jomo Kenyatta University of Agriculture and Technology,
P. O. Box 62000- 00200 Nairobi, Kenya

[3]CSIRO – Tasmanian ICT Centre
GPO Box 1538 Hobart TAS 7001 Australia

ABSTRACT

The purpose of this paper is to study the adoption of information technology security policies in Kenyan Small and Medium Enterprises (SMEs). Particularly this study looks at whether the roles and responsibilities of Information Technology (IT) security in SMEs are well defined, whether SMEs have a documented information security and are if employees aware of the policy. Further the study finds out whether SME employees are given adequate and appropriate information security education and training, and if employees are well informed as to what is considered acceptable and unacceptable usage of the organization's information systems. There is evidence from the survey to suggest that IT security policies are not widely adopted and the benefits harnessed by Kenyan SMEs. The survey reveals that much more needs to be done if SMEs are to realize the benefits of information technology without compromising their security status. This is one of the first studies to explore IT security issues in Kenyan SMEs. The survey is likely to assist SME owners, practitioners, and even academicians gauge how effective their information security efforts have been.

Keywords: *SMEs, Information Security Policy, Kenya, Information Technology Security*

1. INTRODUCTION

We can no longer rely entirely on our traditional security controls- e.g. physical access controls, security guards –to ensure the security of an organization's assets, processes and communications (Tarimo, 2006). The multiplicity of new technical possibilities gives rise not only to new products, services and more efficient and effective of doing things, but also the possibility of misuse of the technology. However, research findings show that, in many cases, security issues come as an-after-thought in the ongoing transformation to ICT-enabled organizational or governmental context (Tarimo, 2006). We argue that unless appropriate measures are put in place by Small and Medium Enterprises (SMEs), dealing with IT security issues will prove to be extremely difficult.

Much like any other business asset, information is an asset that needs to be strategically managed and protected. It is therefore imperative that leaders of organizations and particularly SMEs understand the value of information contained within their business systems and have a framework for assessing and implementing information security. This framework could be in form of and not restricted to a security policy with stipulates among other things the roles and responsibilities of all workers in relation to IT security.

Security of data is critical to the operations of firms. Without the ability to store, process and transmit data securely, operations may be

compromised, with the potential for serious consequences to trading integrity (Clear, 2007). Thus, IT security is likely to become even more important as SMEs continue to harness the benefits of connecting to other networks and particularly the Internet.

The key objective of the survey was to provide some information on the adoption of IT security policies in addressing IT security challenges in Kenyan SMEs. In addressing this issue, this paper is organized into six sections. Following a brief introduction, the next section highlights some information security issues. Section three addresses the research methodology. Section four presents results and analysis. Section five discusses the results in the light of the literature. The last section draws conclusions and future research directions.

2. INFORMATION SECURITY IN SMES

According to Whitman and Mattord (2003), "information security is the protection of information within a business, and the systems and hardware used to store, process and transmit this information". Small and medium-size enterprises represent the spinal code of most European Union countries economies (Grama and Fotache, 2007).

In Kenya, "micro-enterprises" are those with 10 or fewer workers, "small enterprises" have from 10 to 50 workers, and "medium enterprises" have 51 to 100 workers (Gray, 2000).

There is no generally accepted definition of a small and medium business. The most commonly used criteria for defining a small and medium business is number of employees and annual sales (Hashim, 1995). Private companies are often reluctant to disclose their annual revenues (Montazemi, 1988). Thus most researchers choose number of employees as a cut-off point to differentiate between small and medium businesses and larger companies. For the purpose of this study, a small and medium enterprise will be taken a company with full-time employees not exceeding 100.

2.1 EVOLUTION OF SMES IN SECURITY TERMS

According to Earl (2002), the evolution of SMEs in security terms is dependent on Information and Communication Technology (ICT) usage and can be categorized as follows:

- **No usage**: There is no ICT usage or limited usage and therefore security technologies are not required
- **Basic ICT usage**: E-mail and static web pages are implemented within the business; basic security should be implemented such as passwords, secure web mail, antivirus software and configuration of browser settings
- **Intermediate ICT Usage**: E-commerce platforms are being used including online payment systems. An increased level of security is required. Technologies that could be adopted at this stage are Secure Socket Layer (SSL), Digital certificates and secure payment options
- **Advanced ICT usage**: E-business platforms are used including Business to Business (B2B) processes. A high level security is required such as Public Key Infrastructure (PKI), and Virtual Private Networks (VPNs) which allow secure business-to-business communications

It is important that IT security policies in SMEs are reflective of the ICT usage. For instance, in SMEs where there is limited or no ICT usage then there is no need to have an IT security policy. For SMEs with sophisticated ICT usage, there is need to have a policy which addresses all issues about usage of their ICT infrastructure.

SMEs constitute a big portion of developing economies and this can be demonstrated by some of the incentives given to SMEs by governments including start up capital. In Kenya, one source of funding for SMEs is the Youth Enterprise Development Fund (YEDF). According to the YEDF official website (http://www.youthfund.go.ke, 2009), the YEDF is mandated to perform the following among other functions: provide funding and business development services to youth owned or youth focused enterprises; attract and facilitate investment in micro, small and medium enterprises oriented commercial infrastructure such as business or industrial parks, stalls, markets or businesses incubators that will be beneficial to youth enterprises; and support youth micro, small and medium enterprises to develop linkages with large enterprises. This demonstrates the importance of SMEs in Kenya and hence the importance of this study.

2.2 BENEFITS OF AN INFORMATION SECURITY POLICY

According to Mlangeni and Biermann (2006), the process of minimizing risks associated with information security includes the compilation of a detailed and standardized information security policy. Such a policy can among other things define issues such as threats and corresponding countermeasures in addition to defining roles and responsibilities of employees.

Information security policy also specifies the procedures, systems and tools required to protect an organization's information. The benefits of creating such a policy include:

- Responsibilities for the specific tasks involved in protecting your information (for example, reviewing firewall logs, conducting back ups, etc) will have been clearly defined and agreed, thereby ensuring that necessary tasks are actually carried out
- Information security policies will help the business understand exactly what tools and hardware are required for protecting their information. This can be valuable for resource planning and for ensuring that the firm's actual security measures are at an acceptable level
- Information security policies will help protect the business' investment in IT. This is achieved by defining what must be done to ensure all IT assets are adequately protected against damage
- The practice of developing information security policies is becoming increasingly popular and may be considered a source of competitive advantage amongst security conscious business partners and customers (PricewaterhouseCoopers, 2002)

The need for an information security policy in strive towards the securing of information, has been established extensively in both the research and industry fields (Schneier, 2000; Whitman and Mattord, 2004). The question then arises, how many SMEs in Kenya have a well documented IT security policy?

The growth of the Internet as a medium for business and commerce has caused information and systems security to be a growing problem (Dimopoulos et. al., 2004). Security incidents result in financial losses to organizations damage their reputation, disrupt the business continuity and sometimes may also have legal implications (Department of Trade and Industry, 2004). In order to avoid such challenges, organizations should ensure that they are adequately protected, and one of the basic ways to achieving this is developing and adopting a security policy.

3. RESEARCH METHODOLOGY

The different categories of primary data collection methods include laboratory measurements, field observations, archives/collections, questionnaires and interviews (Sharp and Howard, 1998). However, only questionnaires and interviews are suitable for the data required, as the opinions of a large and diverse group of people are needed. Questionnaires provide a more structured way of gathering and recording data. The research entailed a survey of SMEs in Kenya, were primary data was collected by means of a questionnaire. Most of the questions were adopted from previous studies but modified to capture data relevant to the current SME study. These were measured on a five-point likert scale whereby 1 represented "strongly agree" and 5 "strongly disagree". A preliminary version of the questionnaire was discussed with scholars and managers. Some questions were reworded and the original structure of the questionnaire was amended.

This research is based on collected data which is then analyzed and organized to unveil some trends or patterns regarding IT security in Kenyan SMEs. We believe that to be able to address IT security issues effectively in SMEs, it is important to properly understand how IT security is currently being practiced in Kenyan SMEs. SMEs targeted in the survey included those in the consulting, recruitment, vehicles, cleaning, legal, estate agent, medical, equipment leasing/rental, equipment repairs, and any others so long as the organization has got not more than 100 full time employees.

The sample consisted of:

- Formally registered businesses, the informal sector was not considered.
- The telephone directory was used to get regional distribution of SMEs
- Sectoral distribution of SMEs was based on national data from the Central Bureau of Statistics

The researchers administered the questionnaire over a period of four months between October 2009 and January 2010 to SMEs selected from all over Kenya. One hundred and twelve (112) SMEs were randomly identified to participate in the survey. The researchers then contacted the SMEs requesting them to participate in the survey. Those who responded positively were then e-mailed the questionnaire which they were free to fill and e-mail back or they could fill and inform the researchers when to pick. In some cases, the questionnaire was delivered physically by the researchers and picked. The respondents were assured that all personal respondents would remain strictly confidential. Finally, twenty one (21) completed questionnaires were collected.

The respondents included business decision makers, IT managers, or people who take care of computers systems in SMEs. Out of the 21 SMEs that participated in the questionnaire survey, thirteen agreed to post-survey interviews to obtain "richer" information about IT security issues affecting them. As a consequence, in addition to responses to the questionnaire, other useful insights were also gathered. The exact of respondents in terms of nature of business, length of time the business has been in operation, current number of employees, number of computers used in the businesses and how long they have used computers are represented in Table 1 through to Table 5.

Table 1: What is the nature of your business?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Consulting	5	23.8	23.8	23.8
	Computers	3	14.3	14.3	38.1
	Equipment Repairs	2	9.5	9.5	47.6
	Other Professional Service	6	28.6	28.6	76.2
	Recruitment	1	4.8	4.8	81.0
	Vehicle Services	1	4.8	4.8	85.7
	Estate Agent	3	14.3	14.3	100.0
	Total	21	100.0	100.0	

Table 1 shows the nature of the surveyed firms in terms of their operations. Majority of the enterprises are in Consulting and Professional Services.

Table 2: How long has the business in operation?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	2	9.5	9.5	9.5
	2	2	9.5	9.5	19.0
	3	1	4.8	4.8	23.8
	4	2	9.5	9.5	33.3
	5	3	14.3	14.3	47.6
	6	1	4.8	4.8	52.4
	7	2	9.5	9.5	61.9
	8	2	9.5	9.5	71.4
	10	2	9.5	9.5	81.0
	12	1	4.8	4.8	85.7
	14	1	4.8	4.8	90.5
	37	1	4.8	4.8	95.2
	89	1	4.8	4.8	100.0
	Total	21	100.0	100.0	

Table 2 shows the length of time (years) the surveyed SMEs have been in operation. More than 90% of firms surveyed were less than 14 years old.

Table 3: What is your current number of employees?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0-5	4	19.0	19.0	19.0
	11-25	6	28.6	28.6	47.6
	36-50	1	4.8	4.8	52.4
	51-	5	23.8	23.8	76.2
	6-10	5	23.8	23.8	100.0
	Total	21	100.0	100.0	

From Table 3, we note that majority of the SMEs surveyed had 11-25 employees (28.6%), followed by 6-10 employees (23.8%) and 51-upwards (23.8%).

Table 4: How many computers do you use in your business?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	2	9.5	9.5	9.5
	2	1	4.8	4.8	14.3
	3	2	9.5	9.5	23.8
	5	2	9.5	9.5	33.3
	6	1	4.8	4.8	38.1
	7	1	4.8	4.8	42.9
	9	2	9.5	9.5	52.4
	11	1	4.8	4.8	57.1
	14	2	9.5	9.5	66.7
	15	1	4.8	4.8	71.4
	25	1	4.8	4.8	76.2
	35	1	4.8	4.8	81.0
	40	1	4.8	4.8	85.7
	50	1	4.8	4.8	90.5
	60	1	4.8	4.8	95.2
	80	1	4.8	4.8	100.0
	Total	21	100.0	100.0	

From Table 4, it is evident that more than 50% of the surveyed SMEs were using not more than 15 computers in their operations.

Table 5: How long have you been using computers in your business?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	4	19.0	19.0	19.0
	3	2	9.5	9.5	28.6
	4	3	14.3	14.3	42.9
	5	2	9.5	9.5	52.4
	7	3	14.3	14.3	66.7
	8	1	4.8	4.8	71.4
	10	3	14.3	14.3	85.7
	14	1	4.8	4.8	90.5
	15	1	4.8	4.8	95.2
	19	1	4.8	4.8	100.0
	Total	21	100.0	100.0	

19% of the respondents have been using computers in their operations for one year or less while 4.8% have been using computers for 19 years as shown in Table 5.

4. RESULTS AND ANALYSIS

In this section, we present an analysis of the survey that was carried out to track and investigate information security policies in Kenyan SMEs.

To analyze our questionnaire data, we used the Statistical Package for Social Scientists (SPSS) Version 10. Excerpts from SPSS are presented in tabular format in the following section and thereafter discussed for clarity. Despite the many statistical options SPSS offers, we used frequency tables.

Through the interviews we conducted, SMEs pointed out the need for the following to be incorporated in a security enhancing mechanism for SMEs

- Create more awareness programs amongst SMEs and offer them related products to help in protection
- Education on the topic of Internet security
- Hold vulnerability seminars to try and show SMEs what goes wrong in their day to day operations.

Table 6: Information Technology security is an issue that SMEs should be concerned about

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	16	76.2	76.2	76.2
	Agree	3	14.3	14.3	90.5
	Undecided	2	9.5	9.5	100.0
	Total	21	100.0	100.0	

From Table 6, we note that 90.5% believe that IT security is an issue SME should be concerned about. This helps in showing the importance of this survey and why it is necessary to develop solutions geared towards SMEs.

Table 7: Roles & responsibilities for IT security in our organization are well defined

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	4	19.0	19.0	19.0
	Agree	10	47.6	47.6	66.7
	Undecided	3	14.3	14.3	81.0
	Disagree	3	14.3	14.3	95.2
	Strongly Disagree	1	4.8	4.8	100.0
	Total	21	100.0	100.0	

66.7% of the respondents agreed and strongly agreed that the roles and responsibilities for IT security in their organizations are well defined.

Table 8: We have a documented Information Security policy

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	1	4.8	4.8	4.8
	Agree	9	42.9	42.9	47.6
	Undecided	2	9.5	9.5	57.1
	Disagree	6	28.6	28.6	85.7
	Strongly Disagree	3	14.3	14.3	100.0
	Total	21	100.0	100.0	

From Table 8, we note that only 47.6% of respondents agreed and strongly agreed that they have a well documented IT security policy.

Table 9: Staff are aware of our Information Security policy

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	1	4.8	4.8	4.8
	Agree	6	28.6	28.6	33.3
	Undecided	4	19.0	19.0	52.4
	Disagree	8	38.1	38.1	90.5
	Strongly Disagree	2	9.5	9.5	100.0
	Total	21	100.0	100.0	

Despite 47.6% acknowledging that their organizations have well documented IT security policies, only 33.3% agreed and strongly agreed that their staff are aware of the existence of such policies (Table 9). This shows that there are a substantial number of SMEs with well documented policies but whose staff are not aware of the existence of such a policy.

Table 10: All staff are Information Security Educated and Trained

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	1	4.8	4.8	4.8
	Agree	5	23.8	23.8	28.6
	Undecided	5	23.8	23.8	52.4
	Disagree	7	33.3	33.3	85.7
	Strongly Disagree	3	14.3	14.3	100.0
	Total	21	100.0	100.0	

From Table 10, we note that only 28.6% agreed or strongly agreed that their staff are IT security educated and trained. This is consistent with what some SMEs said during our interviews that in order to address IT security issues adequately, they needed IT security education from practitioners and academia.

Table 11: Staff are informed about acceptable use of information systems

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	3	14.3	14.3	14.3
	Agree	8	38.1	38.1	52.4
	Undecided	5	23.8	23.8	76.2
	Disagree	3	14.3	14.3	90.5
	Strongly Disagree	2	9.5	9.5	100.0
	Total	21	100.0	100.0	

More than half (i.e. 52.4%) of SMEs surveyed agreed and strongly agreed that their staff are informed about acceptable and unacceptable use of information systems as indicated in Table 11.

Table 12: Our organization has suffered security breaches in the last 12 months

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No Information security breaches	5	23.8	23.8	23.8
	Suffered some breaches	16	76.2	76.2	100.0
	Total	21	100.0	100.0	

As shown in Table 12, an alarming 76.2% of respondents reported that they had suffered information security breaches. These breaches included but were not limited to:

- Inadvertent breach (e.g. user accidentally deleted files or changed computer configuration)
- Deliberate attack (e.g. hacker/disgruntled staff gained access, deleting or stealing data)
- Asset theft (e.g. software application misplaced causing re-installation delay/costs)
- Equipment failure (e.g. hard drive crashed causing loss of data and business disruption)
- Back up failure (e.g. system restore failure due to corrupt/ inadequate back ups)
- Data theft (e.g. espionage which resulted in data loss and possible legal exposure)
- Site disaster (e.g. fire or flood causing damage to systems and business disruption)
- Copyright infringement (e.g. staff loading pirated software, legally exposing the org.)
- Compliance (e.g. passing on confidential information, legally exposing the organization)

23.8% reported no information security breaches. This may also mean that these respondents were not willing to disclose their organizations' attacks history information to outsiders.

5. DISCUSSION

An information security policy is normally designed to protect organizational assets. It is important for SMEs to have Information security policies in place even if they are only a few months old. The benefits of adopting an IT security policy are cited earlier in the literature.

Our findings reveal that a substantial number of Kenyan SMEs typically lack formally documented security policies. When considering internationally accepted standards such as ISO 17799, a security policy is the essential foundation for successful security strategy, defining issues such as the IT security goals of the organization, what specifications and guidelines need to be followed, and therefore what is acceptable and what is not (Dimopoulos et. al., 2004).

The IT security process starts with a definition of the roles and responsibilities of each employee in relation to IT security. SME management should not assume that their employees know their roles and responsibilities in relation to IT security. Management should make sure that employees are aware of their roles and if possible stipulate these roles and responsibilities in their job descriptions.

SMEs should regularly hold seminars and workshops to sensitize their staff about IT security.

From our findings, it is evident that even SMEs with written security policies in place do not have the policies effectively communicated to all its employees. Effective communication of a security policy to all employees is critically important for it to be enforceable (Casmir, 2005). A technical administrative system must be in place before a system of training and education is adopted, because the formal system provides a framework for the content of the training program (Hagen, 2008).

Our reflection from the analysis of results narrows down to two challenges:

- Lack of management support: Support can be termed as a major obstacle in implementing IT security policies. It's the work of SME management to ensure that the roles and responsibilities for IT

security in their organizations are well defined. Only 66.7% of respondents acknowledged having their roles defined. It is also the work of SME management to ensure or facilitate the development of such policies. SME's are usually born out of entrepreneurial passion and limited funding, with business systems that lack any degree of integration and sophistication (Upfold & Sewry, 2005). Policies and frameworks for information security planning and disaster recovery are usually non-existent.

- Lack of appropriate security training: Appropriate education and training programs help raise the awareness levels of IT security policies (currently at 47.6%) and informing SMEs about what is acceptable and unacceptable use of information systems (currently at 52.4%). Inadvertent threats pose some of the highest information security risk to SME's and yet personnel training and awareness programmes are often neglected (Whitman and Mattord, 2003).

6. CONCLUSION

This study has provided evidence of a major security problem in Kenyan SMEs, and may lead to them experiencing security problems as a result of not implementing basic and necessary countermeasures.

Despite the fact that an IT security policy is a basic IT security tool, Kenyan SMEs appear to be lagging behind in this aspect. From the survey it is evident that some SMEs do not have IT security policies. The length of time an SME has been in operation and how long it has been using computers in its operations are key determining factors to how widely acceptable information security policies are, how employees are sensitized about acceptable and unacceptable usage of information systems, and how effectively SMEs provide adequate and appropriate security training. The younger an SME is the less it adopts security policies, less its employees are sensitized about information security issues, and the less its employees are information security trained.

SMEs are depending more on their IT infrastructure but they lack the means to secure it appropriately due to inadequate know-how. SMEs can be made adequately aware of IT security issues through regular education and training.

Further research can look at ways of assisting SMEs particularly in Kenya come up with comprehensive IT security policies and sensitizing SMEs management about proper IT security frameworks including well articulated IT security standards. There is need for further research to also address issues related to the evolution of ICT usage and their implication to IT security policies.

ACKNOWLEDGEMENT

The authors would like to thank the German Academic Exchange Service (DAAD) for funding this research.

REFERENCES

1. Casmir, R. (2005), A Dynamic and Adaptive Information Security Awareness (DAISA), *Stockholm University, Department of Computer and Systems Sciences*, December 2006.

2. Clear, F. (2007), SMEs, electronically-mediated working and data security: Cause for concern? *International Journal of Business Science and Applied Management*, Vol 2 Issue 2, 2007.

3. Department of Trade and Industry (DTI), (2004), *Information Security Breaches Survey 2004*, Department of Trade and Industry, April 2004.

4. Dimopoulos, V., Furnell, S., Barlow, I. and Lines, B. (2004), "Factors affecting the adoption of IT risk analysis" *In Proceedings of 3rd European Conference on Information Warfare and Security*, Royal Holloway, University of London, UK, 28-29 June 2004.

5. Earl, M. (2002), Evolving the E-Business. Business Strategy Review. *http://www.host.ecom-adviser.au* [12/11/2008]

6. Grama, A. and Fotache, D. (2007), ICT and ERP Applications Challenges in Romanian SMEs

7. Gray, K. R. (2000), Small-scale Manufacturing in Kenya: *Characteristics, Problems and Sources of Finance*

8. Hagen, J. M. (2008), How do employees comply with security policy? *A comparative case study of four organizations under the Norwegian Security Act*.

9. Hashim, S. (1995) Information System success factors in the small and medium enterprises in the Northern Region of Peninsular Malaysia *http://www.lboro.ac.uk/departments/bs/research/example2.pdf* [Accessed 25/10/2009]

10. Kenyan Youth Enterprise Development Fund (YEDF) official website. *http://www.youthfund.go.ke.* [22/3/2010]

11. Mlangeni S. A and Biermann E. (2006), Assessment of Information Security Policies within the Polokwane region: *A Case study. Masters Thesis- Tshwane University of Technology.* Available http://www.tut.ac.za [16/9/2009]

12. Montazemi, A. R. (1988) Factors affecting information satisfaction in the context of the small business environment, *MIS Quarterly* http://www.emeraldinsight.com/Insight/html/Output/Published/EmeraldFullTextArticle/Pdf/0030230801_ref.html [Accessed 29/10/2009]

13. PricewaterhouseCoopers (2002), Interdepartmental Committee on Network and Information Security: *Information Security Awareness Campaign, SME Section*, October 2002

14. Schneier, B. (2000) Secrets and Lies: Digital security in a networked world. *John Wiley & Sons Inc*.

15. Sharp, J. A. and Howard, K. (1998) The Management of a Student Research Project, 2nd Edition. *http://www.hlss.mmu.ac.uk/infocomms/people/staffpub/rjh.doc* [Accessed 12/2/2010]

16. Sunje A. (2006), The role of government in supporting entrepreneurship and SMEs. DEP policy brief No. 4 (2006) *http://www.unece.org/indust/sme/ece-sme.htm* [14/11/2008]

17. Tarimo, C. N (2006), A Social-Technical View of ICT Security Issues, Trends, and Challenges: Towards a Culture of ICT Security- The Case of Tanzania, *Stockholm University, Department of Computer and Systems Sciences*, December 2006.

18. Upfold, C. T. & Sewry, D. A (2005), An Investigation of Information Security in Small and Medium Enterprises (SMEs) in the Eastern Cape.

19. Whitman, M. & Mattord, H. (2003), Principles of Information Security, 1st Edition, *Thomson Learning*, Boston, Massachusetts

20. Whitman, M.E. and Mattord, H.J. 2004. Improving Information Security through Policy Implementation. *In Proceedings of the 7th Annual Conference of the Southern Association for Information Systems.*