ISSN:0975-9646

Information Technology (IT) Security Management in Kenyan Small and Medium Enterprises (SMEs)

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

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

***Abstract*— The aim of this paper is to study the management of Information Technology (IT) security in Kenyan Small and Medium Enterprises (SMEs). Particularly, this study looks at whether SMEs have a designated employee in charge of IT security, whether SMEs seek external expertise about IT security where it is not internally available and if employees are aware that IT security incidents should be reported to management immediately. Further, the study finds out whether SMEs have a formal disciplinary process for employees who violate the company's IT security policies and processes and if their IT security measures have been reviewed within the last year. There is evidence from the survey to suggest that Kenyan SMEs do not have in place proper IT security management practices. The survey reveals that SMEs need to put in place good management and disciplinary measures if they are to realize the benefits of IT security. This is one of the first studies to explore IT security issues in Kenyan SMEs. This survey is likely to assist SME stakeholders gauge the effectiveness of their IT security management structures.**

***Keywords*— Information Technology, Security, Kenya, SMEs, Management**

I. INTRODUCTION

Much like any other business asset, information is an asset that needs to be strategically managed and protected. It is therefore important that leaders of business organizations understand the value of information contained within their business systems and have a framework for assessing and implementing information security.

Small and Medium Enterprises (SME's) are usually born out of entrepreneurial passion and limited funding, with business systems that lack any degree of integration and sophistication [12]. Policies and frameworks for information security planning and disaster recovery are usually non-existent. Inadvertent threats pose some of the highest information security risk to SME's and yet personnel training and awareness programmes are often neglected.

According to Clear [1], there are a number of guides offering advice on "good practice" in relation to data security when working in a distributed and electronically-mediated manner and three are noted here:

- Workers should be trained to protect data security through anti-virus software, password use and taking back ups of work in progress; if such training were not forthcoming, then workers should be held responsible for losses of data
- Safe data handling is dependent not just on technical measures and procedures but also on having reliable and vetted staff.
- Staff should be given guidance on selecting appropriate technology, software packages and tools for best practice in data security to be followed.

We have carried out a survey to provide some information on the management of Kenyan SMEs in relation to it IT security.

II. Information Security in SMEs

According to Whitman and Mattord [14], "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 [3].

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 [4].

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 [7]. Private companies are often reluctant to disclose their annual revenues [10]. 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 is taken to be a company with full-time employees not exceeding 100.

III. Evolution of SMEs

According to Earl [2], the evolution of SMEs in security terms is dependent on 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 management in SMEs is reflective of the ICT usage. For instance, in SMEs where there is limited or no ICT usage then there is no need to have in place IT security management structures. For SMEs with sophisticated ICT usage, there is need to put in place IT security management mechanisms to ensure that their ICT infrastructure is properly secured.

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 [8], 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.

People constitute the least predictable and yet most critical component of any information system. Personnel are what bind the organization together ensuring that practices do not infringe upon legal, regulatory or governance concerns. Part of the leadership challenge remains getting staff to support and participate in the implementation of security systems, policies and practices.

Vroom and Von Solms' [13] suggest establishing a culture of employee co-operation and buy-in through the alignment of organizational and individual values and behaviour. It is important that SME management appraise and train staff so that they remain informed as to the impact their actions may have on their organizations security.

IV. SME Governance

Stakeholders in an organization have a right to IT governance and the protection to information assets, just as they would expect the protection and control of traditional assets such as plant and machinery.

Upfold and Sewry [12] note that governance is likely to be taken seriously in large organizations than in SME's, as management have to answer to stakeholders and boards of directors. As SME's are established and seek to grow, it is essential for management to adopt good management practices, as this is likely to provide vital assurance to potential funders, investors and partners. Good governance

also ensures that policies are addressed, and these directly impact information security.

In managing information security, an organization may piece together its own suite of controls, adopt a code of practice, embrace a security standard and strive for certification, or use a combination of these to ensure that assets are adequately protected [12]. In order to implement standards, a risk assessment should be conducted. On completion of the risk assessment, controls deemed irrelevant are dropped from the standards, while those standards considered necessary and inadequately addressed are then added into the standard. This way, the standards are fine-tuned and customized to meet the security requirements of the organization.

Developing secure systems is not easy most of the time. A solution developed to cater for today's ICT security threats would not necessarily be applicable for tomorrow's threats; because the threats landscape in ICT keep changing all the time, in line with the changes happening due to advancements in the technology itself [11]. This observation underlines the importance of developing not only security solutions, but also methods, structures and processes that may assist in sustaining the security solutions so developed as well as placing the system in equilibrium. The solutions and methods we develop should be able to evolve and adapt to the changing IT needs. This can be achieved through proper IT security management and continuous review of the mechanisms SMEs put in place.

V. RESEARCH METHODOLOGY

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 analysed and organized to unveil some trends or patterns regarding IT security management 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. 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.

VI. Results and Analysis

In this section, we present an analysis of the survey that was carried out to track and investigate information technology security management 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. Among the many statistical options SPSS offers, we used frequency tables.

Table 6: A Director (or equivalent) member of our staff has the responsibility for Information Technology security

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	4	19.0	19.0	19.0
	Agree	4	19.0	19.0	38.1
	Undecided	9	42.9	42.9	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	

From Table 6, we note that only 38.1% of SMEs surveyed have a director or equivalent person in charge of IT security. It is important to have a designated person in charge of IT security if SMEs are to harness the benefits of information technology without compromising their IT security status.

Table 7: Expertise on Information security is available internally, and where not, external advice is sought

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	6	28.6	28.6	28.6
	Agree	5	23.8	23.8	52.4
	Undecided	5	23.8	23.8	76.2
	Disagree	4	19.0	19.0	95.2
	Strongly Disagree	1	4.8	4.8	100.0
	Total	21	100.0	100.0	

52.4% of the respondents agreed and strongly agreed that expertise on IT security is available internally, and where not external advice is sought (Table 7).

Table 8: Third party (outsider) access to our information systems requires approval by a senior manager

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	6	28.6	28.6	28.6
	Agree	4	19.0	19.0	47.6
	Undecided	4	19.0	19.0	66.7
	Disagree	5	23.8	23.8	90.5
	Strongly Disagree	2	9.5	9.5	100.0
	Total	21	100.0	100.0	

From Table 8, less than half (47.6%) of respondents agreed and strongly agreed that outsiders wanting to access their information systems have to seek approval from a senior manager.

Table 9: Staff are aware that security incidents should be reported to management immediately

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	3	14.3	14.3	14.3
	Agree	10	47.6	47.6	61.9
	Undecided	1	4.8	4.8	66.7
	Disagree	6	28.6	28.6	95.2
	Strongly Disagree	1	4.8	4.8	100.0
	Total	21	100.0	100.0	

A substantial number of SMEs (61.9%) agreed and strongly agreed that their staff are aware that security incidents should be reported to management immediately (Table 9). It is important that employees report security incidents to management for appropriate action to be taken.

Table 10: There is a formal disciplinary process for employees who have violated our security policies and processes

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	2	9.5	9.5	9.5
	Agree	5	23.8	23.8	33.3
	Undecided	5	23.8	23.8	57.1
	Disagree	7	33.3	33.3	90.5
	Strongly Disagree	2	9.5	9.5	100.0
	Total	21	100.0	100.0	

Only a third (33.3%) of the respondents agreed and strongly agreed that their organizations have a formal disciplinary process for employees who have violated the company's IT security policies and processes (Table 10).

Table 11: There is a nominated person in our organization who is responsible for managing the business continuity process

		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	5	23.8	23.8	57.1
	Disagree	7	33.3	33.3	90.5
	Strongly Disagree	2	9.5	9.5	100.0
	Total	21	100.0	100.0	

From Table 11, we note that 33.3% of respondents have a nominated person responsible for managing the business continuity process. It is imperative that SMEs manage the business continuity process appropriately to avoid security threats and to continue harnessing the enormous benefits of embracing IT security.

Table 12: Our security measures have been reviewed within the last year

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	2	9.5	9.5	9.5
	Agree	5	23.8	23.8	33.3
	Undecided	6	28.6	28.6	61.9
	Disagree	5	23.8	23.8	85.7
	Strongly Disagree	3	14.3	14.3	100.0
	Total	21	100.0	100.0	

From Table 12, only a third (33.3%) of respondents reported that their security measures had been reviewed within the last one year. Security threats evolve and it is important SMEs review their security measures in conformance with the changing IT security landscape.

VII. DISCUSSION

When an organization implements countermeasures that threaten abusers, its computer abuse problems would be deterred [9]. A person will find it fit to perform a computer crime when he/she perceives the cost of the punishment to be lower than the expected benefits from the criminal activity.

Rewards and punishment are used as a means to control the form and frequency of appropriate/inappropriate security behavior [6]. They become part of the consequences of employees' behaviour either positive or negative. Rewards may include social or personal interaction tools such as competitions, positive feedback, and praise, or more material and economic things, like gifts and awards. Punishment methods also include personal interactions, such as warnings, withholding of certain benefits, and even dismissal, and more material or economic tools, such as fines and other economic sanctions and penalties.

While a system of rewards and bonuses is commonly used in the business world to motivate a high level of performance and productivity, the approach that predominates at present in the information security field is one of threats and punishment [15]. One problem with the punishment approach is that people cannot be punished for problems out of their control. It is not possible to achieve 100 per cent protection against malware propagating on the Internet and IT users will be at risk even though they are careful in surfing the web, opening emails, and using applications, etc. Another problem with the punishment approach is that employees are protective of one another and are reluctant to report their colleagues' minor security violations [5].

We suggest that SMEs should address the following in their quest to proper IT security management:

- Have a designated person in charge of IT security
- Reward good IT security behaviour and punish errant behaviour
- Seek external advice on IT security management where such expertise is not available within the organization
- Constantly and regularly review their IT security mechanisms

VIII. CONCLUSION

SMEs are leaning more on their IT infrastructure but they lack the means to secure it appropriately due to financial restrictions, limited resources, and adequate know-how. Many SME managers believe that IT security in their companies is basically equivalent to having a firewall and updating the antivirus software regularly. Strategic policies, information theft, business continuity, access controls, and many other aspects are only dealt with in case of security incidents. For IT security to be effective, it should take more than putting in place state-of-the-art technical controls. Effectiveness of security controls is dependent on IT security management among other factors.

SMEs may be more often attacked in the future, as large companies become increasingly difficult to hack.

Despite the fact that proper IT security management is crucial to securing IT infrastructure in SMEs, a substantial number of Kenyan SMEs appear not to have put in place IT security management structures. Good IT security management can involve among other things having a designated person in charge of IT security and ensuring that IT security measures are reviewed at least once a year. Further research can look at ways of assisting SMEs put up good and functional IT security management structures.

ACKNOWLEDGEMENT

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

IX. REFERENCES

[1] 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

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

[3] Grama, A. and Fotache, D (2007), *ICT and ERP Applications Challenges in Romanian SMEs*

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

[5] Hagen, J. (2008), "*How do employees comply with security policy?*" A Comparative Case Study of Four Organizations under the Norwegian Security Act.

[6] Hagen, J. M. and Albrechtsen, E. (2009), "*Effects on Employee's Information Security Abilities by E-learning*," Information Management and Computer Security, Vol 17 No. 4, 2009.

[7] 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]

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

[9] Lee, J. and Lee, Y. (2002), "*A Holistic Model of Computer Abuse Within Organizations*", Information Management and Computer Security, Vol. 10. No. 2. (2002), pp 57-63

[10] 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]

[11] 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.

[12] Upfold, C. T. & Sewry, D. A (2005), *An Investigation of Information Security in Small and Medium Enterprises (SME's) in the Eastern Cape*.

[13] Vroom, C. and Von Solms, R (2004), *Towards information security behavioural compliance*. Computers & Security 2004, Vol 23, pp 191-198

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

[15] Wiant, T. L. (2005), "*Information Security Policy's Impact on Reporting Security Incidents*," Computers and Security, Vol 24 No. 6, pp 448-459.