An Analysis of Information Technology (IT) Security Practices: A Case Study of Kenyan Small and Medium Enterprises (SMEs) in the Financial Sector

Leonard Makumbi
MSc student, School of Computing and Informatics
University of Nairobi, Kenya

Evans K. Miriti
Lecturer, School of Computing and Informatics
University of Nairobi, Kenya

Andrew M. Kahonge
Lecturer, School of Computing and Informatics
University of Nairobi, Kenya

ABSTRACT

Organizations of all sizes are now significantly reliant upon information and communication technology for the performance of their business activities. They therefore need to ensure that their systems and data are appropriately protected against security threats. Unfortunately, however, there is evidence to suggest that security practices are not strongly upheld within small and medium enterprise environments.

The purpose of this study was to investigate the information technology security practices in Small and Medium Enterprises (SMEs) in the financial sector in Kenya. In Particular, the study sought to identify the main perceived threats to information security in the organizations and the measures the organizations put in place to protect the information assets from these threats. The study tried to establish if the risk posed by security failures to the organization’s operations was high based on their reliance in IT systems and if the security posture adopted by the organization reflected the level of risk. The study established that the SMEs studied were highly reliant on Information Technology for their business operations hence the risk posed by failure of IT security was high. The study found that the major perceived and experienced threats to security were viruses and system users. The study also found that in the SMEs, there were some attempts at securing the IT assets though these efforts were largely uncoordinated. The IT security role was frequently unassigned, or allocated to someone without appropriate qualification. Most organizations did not have a formally specified IT security budget although some security related expenditures were made.

General Terms

Information Security

Keywords

SMEs, Information Security, Controls, Threats, ICT, Kenya

1. INTRODUCTION

Organizations are becoming increasingly reliant on information technology to fulfill many of their basic functions. The move to a digital economy has caused information and communication technology to become valuable business assets that need to be protected [6]. New security issues such as viruses, hackers, and worms come to light in news articles every day and underline the importance of taking preventative measures.

These are serious threats with serious consequences. Yet, many small businesses have not taken the steps to safeguard their businesses. Usually this may be due to limited resources but in many cases, small business owners are simply unclear as to what steps they should take or even where to start [4]. In a study by [2], about adoption of information security policies by Kenyan SMEs, 76.2% of the respondents indicated that they had suffered information breaches within the previous 12 months. These breaches included: inadvertent breaches by users, deliberate attacks, asset theft, equipment failure, backup failure, data theft, site disaster, copyright infringement, and privacy breaches. They also found that a substantial number of SMEs lacked documented security policies. This lack of adherence to recommended practice could probably explain the high number of reported incidents. This study will differ in that it will look at the controls put in place to counter perceived threats, whether or not there is a documented security policy. The authors in [1] point out that SMEs have a weak understanding of information security, security technologies and control measures, and neglect to carryout risk assessment or develop security policies. They also state that SMEs generally are lacking in the funds and the expertise, and time to coordinate and manage security activities. They also point out that SME owners are not supportive of information security in terms of time and budget. This study also seeks to find out the level of support of SME management to information security.

2. RESEARCH OBJECTIVES

The main objective of this study was to establish the perceived major threats to information system assets in SMEs and the practices put in place to protect the information security assets. This would help in identifying the gaps, which can be used in the sensitization of SME managers on security measures they need to put in place, and possibly assist security service providers in determining the type of security services and products they should be developing and offering to SMEs.

The specific objectives include

i. Establish the level of reliance Kenyan SMEs are on ICT

ii. Establish the most prevalent security threats among Kenyan SMEs

iii. Establish how Kenyan SMEs are protecting their computers, data, and networks from information security risks

3. RESEARCH QUESTIONS

i. To what extent are the selected financial institutions reliant on their ICT systems?

ii. What Are the most prevalent threats to these organizations' Information systems assets?

iii. What measures are organizations putting in place to protect their information system assets against these threats?

4. RESEARCH DESIGN

The purpose of this research is to describe information security issues affecting Kenyan SMEs. The case study approach was selected for this research to enable the researchers get an in depth view of the practices within the selected organizations [3].

4.1 Case Selection

A cross section of organizations was chosen to ensure that the findings could be used to make valid inferences about information security within the financial sector SME's in Kenya. Six SMEs operating in the financial sector were selected. The goal was to focus the research in one sector and in so doing get more information about information security in this sector, rather than getting a little from different sectors. The specific cases were also selected based on their willingness to provide the required information to the researcher. The cases selected were considered typical rather than unique in the financial sector.

The cases selected were:

i. A small financial services company (brokerage firm)

ii. 2 Medium financial services company (investment bank)

iii. 3 commercial banks with between 55-100 employees.

4.2 Data Collection Techniques

In case study research, the researcher uses a variety of data gathering methods to produce evidence that leads to greater understanding of the case and answers the research questions [5]. This also provides the researcher with an opportunity to triangulate the data in order to strengthen the research findings and conclusions.

The following data collections techniques were employed:

i. In-depth interviews

ii. A structured questionnaire

iii. Observation

4.3 Data Analysis

Qualitative analysis of data was employed. The main objective of the analysis was to identify recurring themes in data and group these into categories. The other objective was to find out the importance assigned to the previously identified issues by the organizations. Cross-case analysis was also carried out to determine if there were findings that were common to all the cases.

5. RESULTS

5.1 Case Analysis

Tables 2 to 5 give a summary of the findings in each of the cases investigated

Table 1. Case 1 – Small Financial Services Company (Brokerage Firm)

	Reliance on IT
Main Uses	Email, internet access, sharing files
Level of reliance	The level of reliance is average; but clients do place orders using emails
	Threats
Main Threats	Viruses; hackers; organization's users
Incidents	Viruses; Theft of it resources, destruction of IT resources; unauthorized access by employees; financial fraud; misuse of the internet by employees especially by spending time on social sites
	Counter measures
Strengths	Availability of Security Policy; Firewall; usernames and passwords; offsite and local backups; antivirus
Weaknesses	Lack of awareness on security policy; Security policy not enforced; negligible IS security budget; no dedicated security personnel

Table 2. Case 2 – Investment Bank

	Reliance on IT
Main Uses	Clients can place orders online; all users have PCs used to carry out their routine tasks
Level of reliance	High
	Threats
Main Threats	Hackers; competitors; disgruntled employees; users in general; viruses; lack of knowledge on security issues
Incidents	Information leaks; theft of IT resources; industrial espionage; denial of service; financial fraud; theft of IT resources
	Counter measures
Strengths	Firewalls; Antivirus software is kept up to date; security policies and procedures; business continuity plans and disaster recovery plans; penetration test of the network; reasonable security budget
Weaknesses	Lack of dedicated security personnel

Table 3. Case 3 – Investment Bank

	Reliance on IT
Main Uses	Core business activities; Email access; internet access
Level of reliance	High
	Threats
Main Threats	Hackers; competitors; disgruntled employees; users in general; viruses; partners and suppliers with access to IT resources; External IT contractors with access to systems
Incidents	Viruses; theft or destruction of data; unauthorized access by employees; unauthorized use by contractors, suppliers, and customers; financial fraud; misuse of the internet by employees; website duplication at a different site; blockage of access to data by disgruntled employee
	Counter measures
Strengths	Firewalls; encryption; risk assessments; database of incidents and their resolution;
Weaknesses	Lack of dedicated security personnel

Table 4. Case 4 – Commercial Bank

	Reliance on IT
Main Uses	Core Business Activities; organization branches rely on central servers for services Email access, internet access and banking transactions hence they needed WAN links.
Level of reliance	High
	Threats
Main Threats	Viruses; hackers; disgruntled employees; system users; suppliers or partners with access to their systems;
Incidents	Viruses; misuse of the internet by employees;
	Counter measures
Strengths	Firewalls; antivirus;
Weaknesses	Lack of dedicated security personnel

Table 5. Case 5 – Commercial Bank

	Reliance on IT
Main Uses	WAN connection to branches and other external companies; use of IT by employees for routine operations
Level of reliance	High
	Threats
Main Threats	Viruses; hackers; disgruntled employees; system users; suppliers or partners with access to their systems;
Incidents	Theft of computer assets; unauthorized access;
	Counter measures
Strengths	Firewalls; encryption; usernames and passwords; antivirus; disaster recovery plans; outsourced security experts; large security budget
Weaknesses	Lack of dedicated security personnel

5.2 Cross Case Analysis

In all the cases considered, viruses are seen as a major threat to the Information Assets. System users and in particular disgruntled system users are also seen as a considerable threat. Hackers are also considered a serious threat with all the organizations putting firewalls in place. The cases indicate that there are attempts to develop security policies within these organizations but the implementation is poor. There is also an indication of low budgetary support for IT security within most of the organizations. This could explain the lack of dedicated security personnel within the organizations. The sophistication of security measures put in place seems to increase with the level of reliance of the business on IT systems.

6. DISCUSSION

The results show that there is awareness among the organizations investigated on the importance of Information Systems Security. These organizations have tried to put security measures in place based in their reliance on IT systems. Because of the nature of these organizations, financial fraud seems to feature prominently among the incidents that are reported. Such organizations should put various measures in place including segregation of duties to guard against such risks. Loss of computer assets also seems to be a recurring problem within these organizations. No particular measures seem to have been put in place to guard against this problem. Common controls against this would include physical security controls and inventories of IT assets. Firewalls are the common defense employed against hacking. This is a commendable practices but which can be improved on. One company is noted that they had a hired an external company to perform penetration tests. This is an example that should be emulated by other companies considering security measures can be complicated to put in place and test and an organization may not have the resources to carry out these procedures. System users are also seen as a common threat. This can be ameliorated by awareness campaigns targeted at the users to sensitize them on security matters.

7. CONCLUSION

In summary, this research provided insights into information security in small Kenyan financial institutions context through the investigation of organizational reliance on IT; information security threats; actual incidents; countermeasures; and information security budgets. A qualitative, case based research methodology was used. The study found that there are some attempts to implement some security measures with the amount of effort correlating with the level of reliance of the business on IT. Limited budgets and personnel seem to be a major handicap in the attempts to improve Information systems security.

Further Work in this area could include trying to find out the value of stolen IT resources, the worth of leaked information and if this information has been used by competitors or to the detriment of the organization that lost the information. The value of money lost via financial fraud would also be worth investigating in order to find out the seriousness of the problem. It would also be interesting to investigate organizations in other sectors in order to find out if they face similar or different threats and what counter measures they are putting in place.

8. REFERENCES

[1] Dojkovski, S., Lichtenstein, S., & Warren, M. J. (2007). Fostering Information Security Culture in Small and Medium Size Enterprises: An Interpretive Study in Australia. 15th European Conference on Information Systems, (pp. 1560-1571). St. Gallen, Switzerland.

[2] Kimwele, M., Mwangi, W., & Kimani, S. (2010). Adoption of Information Technology Security: Case Study of Kenyan Small and Medum Entreprises (SMEs). Journal of Theoretical and Applied Information Technology, 18 (2).

[3] Kothari, C. (2004). Research Methodology: Methods and Techniques. Delhi, India: New Age International (P) Ltd.

[4] Microsoft. (2005). Security Guide for Small Business. Microsoft.

[5] Soy, S. K. (2006). The Case Study as a Research Method. Retrieved Oct, 2012, from http://www.gslis.utexas.edu/~ssoy/usesusers/l391d1b.htm

[6] Stoneburner, G., Hayden, C., & Feringa, a. A. (2004). Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A. National Institute of Standards and Technology.