DETERMINANTS OF INFORMATION SECURITY AMONG SMALL AND MEDIUM ENTERPRISES IN KENYA

Simon Ngura

Jomo Kenyatta University of Agriculture and Technology

Dr. Michael Kimwele

Jomo Kenyatta University of Agriculture and Technology

Dr. Gladys Rotich

Jomo Kenyatta University of Agriculture and Technology

CITATION: Ngura, S., Kimwele, M. & Rotich, G. (2015). Determinants of Information Security among Small and Medium Enterprises in Kenya. *European Journal of Business Management, 2* (1), 124-143**.**

ABSTRACT

Figures from Australia, USA and UK, reveals that employee misuse and abuse of Internet services comprise twenty - fifty per cent of all Internet incidents. Companies have identified information security as a key concern. A positive information security culture can aid in minimizing the people threat compromising information security while interacting with IT systems. Statistics from Kenya National Bureau of Statistics (KNBS) shows that SMEs contributes about 70% to the country's GDP and therefore an important segment in the country. SMEs are ranked highest to risk exposure related to information security by PWC. SMEs in Kenya are increasingly reliant on automated and interconnected systems to perform functions essential to their customers' welfare, in sale of goods and services and hence the increase in the information security due to the high dependence on technology. In relation to this, this study sought to establish the effect IT literacy, IT policies, top management commitment and organizational resources as determinants of information security in SMEs in Kenya. To achieve these objectives, this study employed descriptive survey. The population of interest of this study was employees in top 100 SMEs as identified during Kenya's Top 100 SMEs Survey ('Top 100 Survey') conducted in the year 2011. This study used purposive sampling, targeting employees in the IT department in the top 100 SMEs, to get a study sample of

60 respondents. This study collected both primary and secondary data. While a semi-structured questionnaire was used to collect primary data, secondary data was collected from published books, journals, magazines and companies handbook. The study used drop and pick later method to collect data. Prior to the data collection, a pilot study was conducted to allow for pre-testing of the research instrument to increase validity and reliability. The study used both qualitative and quantitative methods of data collection. Further, the study further employed a multivariate regression model to study the relationship between independent variables and the dependent variable. The study found a significant positive relationship between information security and IT literacy, IT policies, top management commitment and organizational resources. The study therefore recommends information security awareness and training program to boost IT literacy. At the same time, the study recommended that the organizations should align their IT policies with organizational goals to make it everyone's' responsibility to achieve information security. Also, the study recommends that policies should be revised from time to time to take into account changes in organization's mission, operational requirements, threats, environment, or deterioration in the degree of compliance. The top management should provides resources to ensure that information security managers attends industry-specific education and executive-level continuing training.

Key words: *Information Security among Small and Medium Enterprises*

Introduction

Diver (2006) highlighted that each organization has its own information security culture similar to every person having his or her own personality. A positive information security culture can aid in minimizing the people threat compromising information security while interacting with IT systems. Highlighting the significance of information security risk are recent figures from Australia, USA and UK, reveals that employee misuse and abuse of internet services comprise twenty - fifty per cent of all internet incidents (AusCERT 2005; CSI/FBI 2005; ISBS 2006). In relation to this, a recent Australian survey, forty percent of respondent companies identified information security culture as a key concern (AusCERT 2005).

According to Besnard and Arief (2004), employees may ignorantly or negligently contribute to information security risks – for example, by unwittingly retrieving spam electronic mail, opening virus e-mail attachments, or dismissing information security threats as unimportant in comparison

with other needs such as usability. Recent survey by McAfee (2005) in an article, "threat within" indicated that; twenty-one per cent of workers allowed family and friends to use company laptops and personal computers for internet access; fifty-one per cent of workers connect their own devices or gadgets to their company personal computer; sixty per cent of workers stored personal content on their company personal computer; ten per cent of workers downloaded prohibited content at work; while sixty per cent of workers stored personal content on their company personal computer. This indicates high company information exposure to risk.

According to Siponen (2007) non-technical issues are as important as technical issues in safeguarding an organization's sensitive information. Technical security controls are strong but they have to be correctly specified, designed, developed, implemented, configured, used and maintained - steps which all involve human beings. Simply put, security-aware managers, staff and information technology professionals make better use of technical security controls (Rotvold, 2008). Protecting information used in the wider context should therefore also incorporate the behavior of people. People manage the information in an organization and interact with information technology systems. In line with this Williams (2009) noted that the human component is a significant factor in information security, with a large number of breaches occurring due to user error. Technical solutions can only protect information so far and thus the human aspect of security has become a major focus for discussion. Therefore, it is important for organizations to create a security conscious culture. Hence, a positive information security culture can aid in minimizing the people threat compromising information security while interacting with information technology systems (Eloff and Von Solms, 2000).

In another study by Tarimo *et al.* (2006) conducted in Tanzania, it is found that there is lack of personnel and resources to support information security education at colleges and universities that is one reason for lack of information security culture. Hence the study revealed that cultivating security culture is neither simple nor easy and information security is not an issue that could be addressed entirely by organizations alone; rather, many factors outside the scope of an organization have to be considered. Alnatheer & Nelson (2009) have also highlighted the importance of information security management factors and cultural factors in Saudi Arabia and the study disclosed a gap in terms of addressing the influences of both Information Security Management factors and cultural factors on the adoption of security culture in Saudi Arabia context.

In response to the heightened information security risk that companies are exposed to, many companies have developed an interest in cultivating intuitive — rather than enforced — employee adherence to information security policy, processes and procedures (Dhillon 2001). Such companies are interested in the institutionalization of information security practices as information security culture. The potential value of adopting a socio-cultural approach to information security management was recently highlighted by Galletta and Polak (2003). Their study revealed that peer and supervisory culture may be highly influential in the management of internal internet misuse and abuse. However, while progress has been made globally in the enculturation of information security, more is needed (Ernst & Young 2006).

Lichtenstein and Swatman (2001) and Schlienger and Teufel (2003) recommends various approaches based on policy, awareness, training and education to assist companies in establishing an information security culture. However, managerial initiatives alone will not significantly influence employee behaviour (Rosanas & Velilla 2005) and new conceptual frameworks are needed that identify and integrate complex behaviour modification and cultural change. Supporting the need for further research in this area, the Editor-in-Chief of the respected *Computers & Security* journal observed recently that the human factor in information security deserves greater research attention (Schultz, 2005).

In Kenya, SMEs are increasingly reliant on automated and interconnected systems to perform functions essential to their customers' welfare, in sale of goods and services. However, the factors that benefit SMEs operations—speed of processing and access to information—also increase the risks of computer intrusion, fraud, and disruption. According to PWC (2011), high dependence on technology is ranked highest among the risks by businesses in Kenya. Information systems have long been at some risk from malicious actions or inadvertent user errors and from natural and man-made disasters. SMEs' systems in Kenya are increasingly becoming more susceptible to these threats because computers have become more interconnected and, thus, more interdependent and accessible to a larger number of individuals. In addition, the number of individuals with computer skills is increasing, and intrusion, or "hacking," techniques are becoming more widely known via the Internet and other media. These intrusions and other forms of information security threats among the SMEs in Kenya leads to organizational information leakage to competitors, loss of clients and other stakeholder's information and at other times may lead to distortion of information.

Information Security in SMEs

SMEs are companies the personnel numbers of which fall below a certain limit. Small enterprises outnumber large companies by a wide margin and also employ many more people. SMEs are also said to be responsible for driving innovation and completion in many economic sectors. In Germany, SMEs are defined with a limit of 255 employees; in Belgium, a limit of 100 employees; while in Europe, Micro-entities are companies with up to 10 employees, Small companies – employ up to 50 workers while Medium- sized enterprises have up to 250 employees. In Kenya, micro enterprises are those with 10 or fewer workers, small enterprises have from 10 to 50 employees and medium enterprises have 51 to 100 workers. Micro enterprises comprise the lion's share of enterprises in Kenya while there are a few medium enterprises (Abwao 2002).

Kenya's informal sector compromises of small and medium sized indigenous and family owned businesses. There are more than 800,000 small, medium and micro-enterprises in the country, absorbing about a quarter of the labor force of 30 million people. The emergence of high skill and technology-intensive SMEs has recently been noted, especially in high technology industries (GOK, 2005).

Experts suggest that small and medium size enterprises (SME) are particularly disadvantaged in the development of secure employee behaviour as their information assets are least protected (Taylor & Murphy 2004). SMEs in developing countries generally have a weak understanding of information security. According to Gupta and Hammond (2005), security technologies and control measures, and neglect to carry out risk assessments or develop security policies. This may be because SMEs lack the funds, time and specialized knowledge to coordinate information security or offer adequate information security awareness, training and education (Furnell *et al*. 2000). Majority of those who run SMEs are ordinary lot whose educational background is lacking. They may not be well equipped to carry out managerial routines for their enterprises (King & McGrath, 2002).

Studies indicates that SME owners are not supportive of information security in terms of budget or time, thus impacting the level of security awareness and security technology. For instance, Johnson and Koch (2006) recently found that home-based SMEs would not pay for security. Also, Gupta and Hammond (2005) while SMEs often use power surge protectors; they are unlikely to deploy encryption, firewalls, access control technologies and dial-back modems. Gupta and

Hammond further point out that, lacking specialized knowledge of security technologies, SMEs often retain the security technologies with which they are already familiar and which therefore offer immediate convenience. Further, by giving higher prioritization to other business tasks, SMEs only rarely review their information security needs.

SMEs' capacity to meet growing customer expectations is based largely on their ability to innovate and deliver new products at competitive prices. To do this, the SMEs need to protect their information. SMEs have the ability to innovate effectively and develop new products more rapidly than larger firms. However, many SMEs in Kenya still fail to offer adequate security to their information, which it looses to their competitors, an advantage, adopted by larger firms. This therefore calls for a need to develop information security culture through adherence to IT policies and regulations, qualified employees, positive organization culture and high level of management support and commitment.

Statement of the Problem

Statistics from Kenya National Bureau of Statistics (KNBS) shows that SMEs contributes about 70% to the country's GDP (GOK, 2012). According to government statistics, the SME segment in Kenya contributes over 80% of the countries employment with majority of new jobs being created in that sector (430,000 out of 503,000 new jobs created in 2011). Therefore, SMEs is an important segment in the country. Further, data from World Bank (WB) Kenya shows that, the SME's sector experienced 18% growth rate in the year 2011 (World Bank, 2012).

However, reports from Price Water House Coopers (PWC) ranked SMEs highest to risk exposure related to information security (PWC, 2011). Consequently, United Nation (UN) report indicates that the higher exposure to risk for the SMEs leads to high collapse rate (UN, 2012). High collapse rate leads to loss of job and hence low economic development to the country (GOK, 2013). According to PWC (2011), high dependence on technology is ranked highest among the risks by businesses in Kenya.

However, despite these risks, SMEs have not put in place adequate measures to counter the risks. Knapp *et al.,* (2006) noted that management of security risks is still not prevalent and not comprehensive in the training in most organizations as their lack adequate management support.

Further, SMEs fails to allocate adequate resources and IT policies to counter the risks. This indicates that there are still a lot to be done to curb information insecurity in SMEs in Kenya.

Many empirical researches have been done in the area of information security. Dojkovski, Sneza, Sharman and John, (2010) did an interpretive study in Australia on fostering information security culture in small and medium size enterprises. Also, in Ethipoia, Gebrasilase and Lessa (2011) did a study to ascertain the nature of information security culture in public hospitals in Hewassa. In Kenya, Kimwele, Mwangi & Kimani (2011) conducted a study on Information Technology (IT) Security Framework for Kenyan Small and Medium Enterprises (SMEs). However, despite the massive inquiry into information security, none of these studies has been done to establish the role of IT literacy, IT policies and regulations, top management commitment and organization's resources as determinants of information security in SMEs in Kenya.

Objectives of the Study

The objective of the study was to establish determinants of information security culture among SMEs in Kenya.

Specific Objectives

The study was guided by the following specific objectives;

i. To establish the influence of IT literacy as a determinant of information security among SMEs in Kenya.

ii. To find out the role of IT policies as a determinant of information security in Kenyan SMEs

iii. To find out the influence of top management commitment as a determinant of information security in Kenyan SMEs

iv. To establish the influence of organizational resources as information security determinant in SMEs in Kenya.

Justification of the Study

By having an effective organizational information security culture where employees intuitively protect corporate information assets, small and medium size enterprises (SMEs) could improve information security. Therefore, this study would help SMEs in Kenya and other organizations

alike, as it highlights key challenges of promoting a behavioral and learning approach to information security to complement traditional technological and managerial approaches for SMEs. The study would therefore make recommendations to counter the challenges for a successful development of information security culture in the organizations.

Further, the management and owners of the SMEs, as well as other organizations (big and small), would benefit from this study from adopting a risk-based approach to information security and would be educated about the potential strategic role of information technology and information security.

To the government, through the relevant ministries, and other players in the information technology arenas, the study would be of value, as it provides a guideline that can be used in policy formulation to be followed by other institution willing to institute a culture of information security. Through identification of key elements that support development of information culture and the likely challenges, the regulators would provide a fit all guideline to implementation of information culture guided by this studies findings.

This study would also be of value to scholars. This is because, it adds to the existing pool of reference material in the field of information security. Further, the study would form basis for further research on the gaps that were identified and recommended for further research.

Scope of the Study

The study was conducted in SMEs operating in Nairobi CBD. Employees in manufacturing, retail and trade and service SMEs will be the key respondents to this study.

Limitation of the Study

The researcher however expects some hindrances while conducting the study. The researcher anticipated low generalizability of finding, where the findings could not be used to present a general picture of state of SMEs in Kenya. However, to mitigate this, the study selected adequate sample that is scientific, conforms to law of large numbers and central limit theorem whereby a sample of 30 cases is considered normally distributed. Therefore a sample of 60 respondents was adequate. With these, generalizations were made assuming that the sample is large enough and scientifically selected.

The researcher further anticipated uncooperative respondents. To counter this challenge, the study assured the respondents of confidentiality of information that they gave and that the information they gave would be used for academic purposes and where applicable may influence policies that would have positive implications on information security in their organizations.

The researcher anticipated that the respondents may be biased in giving out information or giving guarded responses which would compromise the study's objectivity and reliability. This limitation was overcome by explaining to the sampled population the essence of the study. Further, the researcher assured the respondents that no one would be victimized on the information that they gave.

LITERATURE REVIEW

Cognitive Learning Theory

This theory states that humans generate knowledge and meaning through sequential development of an individual's cognitive abilities, such as the mental processes of recognize, recall, analyze, reflect, apply, create, understand, and evaluate. The Cognitivists' (Piaget 1976; Bruner 1960; Bruner 1966) learning process is adoptive learning of techniques, procedures, organization, and structure to develop internal cognitive structure that strengthens synapses in the brain. The learner requires assistance to develop prior knowledge and integrate new knowledge. The purpose in education is to develop conceptual knowledge, techniques, procedures, and algorithmic problem solving using Verbal/Linguistic and Logical/Mathematical intelligences. The learner requires scaffolding to develop schema and adopt knowledge from both people and the environment. The educators' role is pedagogical in that the instructor must develop conceptual knowledge by managing the content of learning activities.

Theory of planned behavior

This theory of planned behavior is a theory about the link between beliefs and behavior. The concept was proposed by Ajzen (1991) to improve on the predictive power of the theory of reasoned action by including perceived behavioural control (Ajzen, 1991). It is one of the most predictive persuasion theories. It has been applied to studies of the relations among beliefs, attitudes, behavioral intentions and behaviors in various fields such as advertising, public relations, advertising campaigns and healthcare. The theory states that attitude toward behavior, subjective

norms, and perceived behavioral control, together shape an individual's behavioral intentions and behaviors. In relation to the study, this theory can be used to explain employees' intention to abide by IT policies to ensure information security in their organization. This is because the policies put in place would predict how the employees handle IT resources in an organization.

Three-Component Model of Commitment

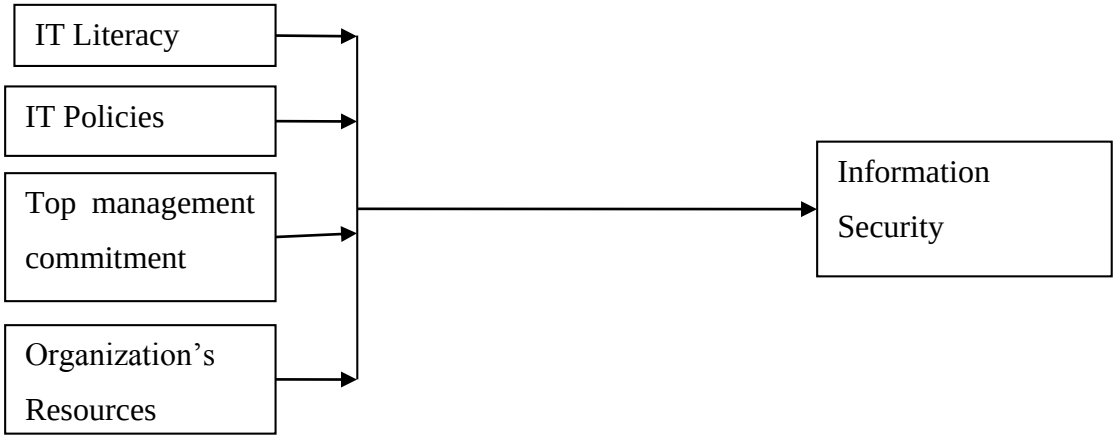
This model was proposed by Allen and Meyer in 1990. This model proposes that organizational commitment is experienced by the employee as three simultaneous mindsets encompassing affective, normative, and continuance organizational commitment. Affective Commitment reflects commitment based on emotional ties the employee develops with the organization primarily via positive work experiences. Normative Commitment reflects commitment based on perceived obligation towards the organization, for example rooted in the norms of reciprocity. Continuance Commitment reflects commitment based on the perceived costs, both economic and social, of leaving the organization. This model of commitment has been used by researchers to predict important employee outcomes, including turnover and citizenship behaviors, job performance, absenteeism, and tardiness (Meyer et al., 2002). Meyer and Allen (1997) provide a comprehensive overview of the theoretical lineage of this model. However, in this study, the model is used to predict employees' behaviors towards information security in an organization based on the level of top management commitment.

Resource-Based Theory

Resource-based theory (Barney, 1991) is used to provide a theoretical foundation to explore the antecedents that affect system quality and service. This theory suggests that organizational resources that are costly or hard to imitate help organizations retrieve competitive advantage. In the case of this study, competitive advantage is looked at in terms of information security culture. One resource-based research stream has considered the functional capabilities of IS as the source of competitive advantage (e.g., Bharadwaj, 2000). Another perspective has focused on how resources are channeled and utilized to bring competitive advantage (e.g., Ravichandran & Lertwongsatien, 2005). However, both streams agree that resource availability determines information security capabilities and further affects organizational performance (Ray, Muhanna & Barney, 2005).

Conceptual Framework

The conceptual framework shows the relationship between the independent variables and dependent variable distilled from the literature review by the study as shown on the figure 2.1 below. It assumes that the relationship between the independent variable and dependent variable is linear, though moderated by government policies and regulation



Independent Variable **Moderating variable** **Dependent Variable**

Figure 2.1: Conceptual Framework

Summary

Fostering information security culture is not an easy task and is faced by a myriad of challenges. However, the issue of information security is becoming more and more crucial in today's information age. This chapter has reviewed past literature relevant to the study. From the literature, employee capacity has been identified as a key recipe to attaining information security. In this regard it is indicated that employees must be qualified to perform a job in order to meet expectations. Information security problems in organizations have been linked to employee behavior. Training to enhance the skills and knowledge should be incorporated in employee development. High-qualified employees are less likely to expose the institution to information risks. Information security culture requires imbedding security and protection considerations into organization culture and management mind-set. Information security can be created in a company

by instilling the aspects of information security to every employee as a natural way of performing his or her daily job.

Top management support is regarded as most important factor affecting information security management activities in organizations. Information security incidences are costly to the organization therefore, the management must take information security culture fostering seriously. The management is involved in decision-making and therefore does the resource allocation in development of information security culture. Organizational policy influences and determines employees' course of action. Appropriate use of computer and network resources, appropriate password habits etc., in an organization are often dealt through organizational computer security policies. Failure to establish information security policies can disrupt business operations and deteriorate organizational reputation and competitiveness as well as that of its customers.

RESEARCH METHODOLOGY

Research Design

Kombo and Tromp (2006) define research design as the scheme outline or plan that is used to generate answers to research-to-research problems. This study employed descriptive survey. A descriptive study attempts to describe or define a subject, often by creating a profile of a group of problems, people, or events, through the collection of data and tabulation of the frequencies on research variables or their interaction as indicated by Cooper and Schindler (2003). This study aimed to establish the state of affairs in information security in SMEs in Kenya. It was focused on determining factors to ensuring information security. Therefore, the study sought to establish the determinants of information security culture in SMEs in Kenya.

Data Analysis and Interpretations

Model Summary

Table 4.1: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate

1	0.919	0.845	0.789	0.6273

Source: Researcher (2014)

The four independent variables that were studied, explain only 84.5% of the information security as represented by the R^2. This therefore means that other factors not studied in this research contribute 15.5% of the information security. Therefore, further research should be conducted to investigate the other factors (15.5%) that affect information security in SMEs in Kenya.

ANOVA Results

Table 4.2: ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	2.534	3	1.267	9.493	.0209[a]
	Residual	9.307	53	2.327		
	Total	11.841	56			

Source: Researcher (2014)

The significance value is 0.0209 which is less that 0.05 thus the model is statistically significance in predicting how IT literacy, IT policies, top management commitment and organizational resources influence information security among SMEs in Kenya. The F critical at 5% level of significance was 2.774. Since F calculated is greater than the F critical (value = 9.493), this shows that the overall model was significant.

Coefficient of determination

Table 4.3: Coefficient of determination

	Unstandardized Coefficients		**Standardized Coefficients**		
Model	**B**	**Std. Error**	**Beta**	**t**	**Sig.**

1	(Constant)	1.207	1.2235		1.615	0.367
	IT Literacy	0.752	0.1032	0.152	4.223	.0192
	IT policies	0.687	0.3425	0.054	3.724	.0239
	Top Management Commitment	0.545	0.2178	0.116	3.936	.0251
	Organizational Resources	0.439	0.1937	0.263	3.247	.0454

Source: Researcher (2014)

Multiple regression analysis was conducted as to determine the relationship between information security and the four variables. As per the SPSS generated table above, the equation ($\mathbf{Y = \beta_0 + \beta_1X_1 + \beta_2X_2 + \beta_3X_3 + \beta_4X_4 + \varepsilon}$) becomes:

$Y= 1.147+ 0.752X_1+ 0.687X_2+ 0.545X_3+ 0.439X_4$

According to the regression equation established, taking all factors into account (IT literacy, IT policies, top management commitment and organizational resources) constant at zero, information security will be 1.207. The data findings analyzed also shows that taking all other independent variables at zero, a unit increase in IT literacy will lead to a 0.752 increase in information security; a unit increase in IT policies will lead to a 0.687 increase in information security, a unit increase in top management commitment will lead to a 0.545 increase in information security and a unit increase in organizational resources will lead to a 0.439 increase in information security. This infers that IT literacy contribute most to the information security followed by IT policies. At 5% level of significance and 95% level of confidence, IT literacy had a 0.0192 level of significance, IT policies showed a 0.0269 level of significance, top management commitment showed a 0.0251 level of significance, and organizational resources showed a 0.0454 level of significance hence the most significant factor is IT literacy.

Conclusion

The study sought to establish the influence of IT literacy as a determinant of information security among SMEs in Kenya. To this objective, the study concludes that IT literacy influences information security in the top 100 SMEs to a great extent. The study showed that experience with IT systems, IT resources literacy and IT skills literacy were elements of IT literacy that influenced information security in SMEs in Kenya. In acknowledgement of importance of IT literacy as a critical element of information security, it was established that the SMEs conducts competency assessment that helps employees improve their IT skills and direct organizations to renovate functions, courses, and strategies and thus nature an information security culture. Also, the SMEs studied were indicated to employ IT literate individuals in the IT department.

On the role of IT policies as a determinant of information security in Kenyan SMEs, the study concludes that IT policies are determinants of information security in organisations. To this end, most of organisations studied had put in place IT policies to enhance information security. In the SMEs studied, efforts are put in place to ensure that policies to aid information security are followed. This ensures that employees in the SMEs comply with information security procedures and policies laid down. IT policies in the SMEs studied were indicated to be crystal clear, these policies ensures confidentiality, integrity, availability, and better control of information assets. Most of SMEs have in place policies that forbid use of company's computer and Internet resources for personal use. Further, in realisation of the dangers that information insecurity has on organisation, the SMEs have adapted training policies for all employees who handle computers and Internet resources to ensure reduction of company's exposure to information security.

The study has concluded that the top management commitment influences information security in Kenyan SMEs to a great extent. Top management in the SMEs play an important role in expediting the implementation of information system security initiatives as well as bringing ISM alignment with the corporate objective and strategies. The top management's support is responsible for initiating awareness and training programs, committed to the Information Security Policy. Top management facilitates education and training for employees to ensure awareness on information asset protection while ensuring consistent enforcement of information security policies and standards.

Further, the study concluded that organizational resources influences information security in SMEs in Kenya to a great extent. The organizational resources established to influence information security in the SMEs include human resource, specialized knowledge, computer and Internet resources and financial resources. The SMEs conducts constant training to develop human resource on areas of information security and also hires qualified human resource to ensure information security. SMEs also make budgetary allocations aimed at improving level of information security.

The study also concludes that there is a positive relationship between information security and IT literacy, IT policies, top management commitment and organizational resources. All factors had a significant p-value ($p<0.05$) at 95% confidence level. The most significant factor was established to be IT literacy, followed by IT policies then top management commitment while organizational resources was the least significant among the factors.

Recommendations

The study established that information security awareness and training program is a critical component of the information security program. It is the vehicle for disseminating security information that the workforce, including managers, needs to do their jobs. Therefore, the study recommends that training programs should be conducted to ensure that personnel at all levels of the organization understand their information security responsibilities and that they properly use and protect the information resources entrusted to them. Creating awareness offers a blended solution of activities that promotes security, establishes accountability, and informs the workforce of security concerns. Training strives to produce relevant and needed security knowledge and skills within the workforce. Training supports competency development and helps personnel understand and learn how to perform their security role.

The study recommends that organizations should make IT policies that align information security with the organization's objectives and make it everyones responsibility to achieve information security. Information security is frequently perceived as the responsibility of the information security department. This perception is generally perpetuated through information security initiatives being funded as stand-alone projects and the failure to inform employees of their role in the protection of information and intellectual property assets. Also, the study recommends that the

information security status associated with high-risk legal and regulatory compliance should be monitored at the executive level to ensure that appropriate priority is given to risk management initiatives.

An information security strategy that is aligned with the company's risk management and corporate governance requirements should be developed and implemented. Further, organization policies put in place should seek to ensure that each line of business that "owns" information requiring specific levels of confidentiality, integrity and availability should designate a liaison to work with the information security manager to ensure that requirements are properly reflected and prioritized in the information security strategy.

Further, the study recommends that over time, information security efforts should be revised based on changes in organization's mission, operational requirements, threats, environment, or deterioration in the degree of compliance. Periodic assessments and revision can be a valuable means of identifying areas of noncompliance and addressing them. Executives should ensure a life-cycle approach to compliance by monitoring the status of their programs to ensure that ongoing information security activities are providing appropriate support to the organization; policies and procedures are current; and security controls are accomplishing their intended purpose.

The study recommends that top management should communicate consistently that every employee is accountable for information security by ensuring that expectations are clearly communicated in the company's information security policies and standards, and consistently demonstrate that violations will not be tolerated. The top management should ensure that every employee, including management, attends an information security awareness update annually and new employees should be appropriately informed of the company's information security concepts and practices.

The study also recommends that senior management in the SMEs should require that all requests for technology expenditures include technology risk identification and risk mitigation requirements as part of the cost-benefit analysis, project objectives, deliverables and funding request. Further, the study recommends that the top management provides funds to ensure that information security managers attends industry-specific education and executive-level continuing

training to increase their understanding of the business information security related risks and enhance their skills in addressing these challenges.

REFERENCE

Admiraal, W., & Lockhorst, D. (2009). E-learning in small and medium-sized enterprises across Europe-Attitudes towards technology, learning and training. *International Small Business Journal, 27*(6), 743-767.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50 (2), 179–211.

Alnatheer, M. & Nelson, K. (2009). Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context. *Proceedings of the 7th Australian Information Security Management Conference*, Perth, Western Australia.

Appari, Ajit & M. Johnson, Eric (2010) Information security and privacy in healthcare: current state of research. *Int. J. Internet and Enterprise Management, Vol. 6, No. 4.*

Armstrong, C. & Sambamurthy, V (2001). Information Technology Assimilation in Firms: the influence of senior Leadership and IT infrastructures System Research, 10 (4), 304-327.

AusCERT (2005) 2005 *Australian Computer Crime and Security Survey*, AusCERT.

Avdjieva, M., Callagher, L., Knight, C., & Mitchell, L. (2004, September). Infolit: A "home grown" information literacy initiative in a flexible e-learning environment. *Paper presented at the Library & Information Association of New Zealand Aotearoa (LIANZA) Conference*, Auckland, New Zealand.

Besnard, D. & Arief, B. (2004) Computer Security Impaired by Legitimate Users, *Computers & Security*, 23, 253-264.

Braun, N. M. (2004). Critical thinking in the business curriculum. *Journal of Education for Business, 79*(4), 232–236.

Bridget, S., and Lewin, C. (2005). *Research Methods in the Social Sciences*. London: Sage publications Inc.

Bruner, J.S. (1960). *The process of education*,. Cambridge, MA: Harvard University Press.

Bruner, J.S. (1966). *Toward a theory of instruction*. Cambridge, MA: Belkapp Press.

Cameron, K. S., & Quinn, R. E. (1999). *Diagnosing and Changing Organizational Culture*. Reading: Addison-Wesley.

Chan, M. Woon, I. Kankanhalli, A. (2005). Perceptions of information security at the workplace: linking information security climate to compliant behavior, *Journal of Information Privacy and Secu*rity 1 (3), 548 – 76.

Computerized Manufacturing Automation (1984). Employment, Education and the Workplace, Washington, *US Congress of Technology Assessment*, OTA CIT-235 April, page 234

Conner, B. *et al*., (2004), Business Software Alliance

Cooper, D. R., and Schindler, P. S. (2003). *Business Research Methods* (8th edn). McGraw-Hill: New York.

Cronbach, L. J. (1971). *Test validation*. In R. L. Thorndike (Ed.). Educational Measurement (2nd Ed.). Washington, D. C.: American Council on Education.

CSI/FBI (2005) Tenth Annual CSI/FBI Computer Crime and Security Survey, *Computer Security Institute*, USA.

Czerniewicz, L., & Brown, C. (2009). A study of the relationship between institutional policy, organisational culture and e-learning use in four South African universities. *Computers & Education*, *53*, 121-131.

Denison, D. R. (1990). *Corporate Culture and Organizational Effectiveness*. New York: Wiley (New York).

Dhillon, G. (2001). Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns. *Computers & Security*; Vol.20, No.2, pp.165-172.

Dhillon, G. & Torkzadeh(2006). Value-focused assessment of information system security in organizations. *Information Systems Journal*,

Dojkovski, S., Lichtenstein, S., & Warren, M. J. (2001) Fostering Information Security Culture in Small and Medium Size Enterprises: An Interpretive Study in Australia*Proceedings of the 3rd Australian Information Security Management Conference*, Perth Australia.

Eisenhardt, K. M. (1989). Agency theory: an assessment and review, *Academy of Management Review*,14 (1)

Eloff, M., M., & Solms, S., H. (2000). Information Security management: A Hierarchical Approach for various frameworks. *Computer & Security*, 19(3), 243-256.

Ernst & Young (2006) *2006 Global Information Security Survey*, Ernst & Young.

Feast, V. (2003). Integration of information literacy skills in business courses. *Reference Services Review, 31*(1), 81–95.

Furnell, S. M., Gennatou, M. & Dowland, P.S. (2000). Promoting Security Awareness and Training within Small Organisations, in *Proceedings of the 1st Australian Information Security Management Workshop*, Deakin University, Geelong, Australia.

Galletta, D.F. & Polak, P. (2003). An Empirical Investigation of Antecedents of Internet Abuse in the Workplace, in *AIS SIG-HCI Workshop*, Seattle, December, 2003

Garoupa, N. (2000). Corporate criminal law and organization incentives: a managerial perspective, *Managerial and Decision Economics*, 21

Gebrasilase, Temesgen and Lessa, Lemma Ferede (2011). Information Security Culture in Public Hospitals: The Case of Hawassa Referral Hospital, *The African Journal of Information Systems*, 3(3:1).

Hu, Q. Hart, P. & Cooke, D. (2007). The Role of External Influences in Organizational information Security Practices: An institutional Perspective. Journal of Strategy information System 16(2), 153- 172.

ISBS (2006). Information Security Breaches Survey 2006, *Department of Trade and Industry*, UK.

Ismail, N. A. (2008). Information Technology governance, funding and Structure: A case analysis of Public University in Malaysia. 25(3), 145-160