TECHMIND RESEARCH
ISSN: 2292-1648
International Journal of Management Excellence
Volume 3 No.1 April 2014

Challenges Facing Information Systems Security Management in Higher Learning Institutions: A Case Study of the Catholic University of Eastern Africa – Kenya

Dr. Bichanga Walter Okibo[1],Mrs. Obara Brigit Ochiche[2]
[1]Jomo Kenyatta University of Agriculture and Technology, Nairobi,Kenya
[2]The Catholic University of Eastern Africa,Nairobi, Kenya
[1]walter.okibo@yahoo.com
[2]obara.brigit@gmail.com

Abstract- *With the popularity of internet applications, many organizations are facing unprecedented security challenges. Security techniques and management tools have caught a lot of attention from both academia and practitioners. However, there is lacking a theoretical framework for the challenges facing information security management in higher learning institutions. Thus this research looked into the challenges facing information systems security management in higher learning institutions. The study was guided by understanding the major challenges facing Information Systems Security Management and establishing the extent of the use of Information Systems Security Management in higher learning institutions. The study used descriptive survey design. It targeted information systems projects managers, administrators or top management and other users (staff) of the systems in key departments. Systematic sampling strategy was used. Descriptive statistics of SPSS were used to analyze the data. Factor analysis technique was used to identify the major challenges that affect management of an institution's information system security. Pearson's Chi-Square was used to test the relationships that exist between the categorical variables. The study found out that system vulnerability, computer crime and abuse, environmental security and financial backing/security are key challenges institutions of higher learning are experiencing in the management of their information systems. The study recommends the implementation of new policies and procedures to guide information system security. Programs for monitoring and evaluating information systems security in relation to performance indicators should be put in place. Institutions should invest heavily in developing their staff through training programmes such as seminars, workshops and conferences to further develop staff skills and abilities on information systems security issues.*

Keywords- *Challenges; Information Systems Security; Higher learning Institutions; Performance Indicators;Management and Internet*

1. INTRODUCTION AND BACKGROUND OF THE STUDY

Information is one of the most important assets of an organization. For any organization, information is valuable and should be appropriately protected (Sitaraman &Venkatesan, 2006). With the serious threat of unauthorized users on the internet, Information System Security (ISS) is facing unprecedented challenges and effective Information System Security Management (ISSM) is one of the major concerns (Eloff &Solms, 2000). Criminals, terrorists, disgruntled employees, technical problems and many other issues can threaten the security and integrity of information systems (Nissenbaum, 2005). Given the importance of information stored in these systems, it is reasonable to believe that information systems security should be an important managerial concern, as much of the literature suggests (Siponen, 2005). ISS is perceived as a way of fighting and preventing criminal activities (EC, 2007). Hacking, malware and viruses constitute problems that security needs to address (Broucek & Turner, 2003). This links ISS with law enforcement and in particular with digital forensics (Sitaraman &Venkatesan, 2006). There are numerous challenges in maintaining security in higher learning institutions (Doherty & Fulford, 2006). First and foremost information security challenge in higher education is limited budgets especially in today's economy. Another challenge is the cultural adaptation to academic information security management. Higher education environments typically have several departments that utilize information technology in separate fashion; from faculty to students; deans to VCs of academic affairs; each has the challenge with balancing information security and an end-user happiness. It's practically impossible given all the pressure. Universities are relying in information systems to carry out their day to day operations. More specifically is the use of Academic Management Systems (AMS) by numerous universities for their business operations including teaching, student administration, research and development. Information security application to university's ISs is strategically important to

maintaining overall business continuity. The ever emerging threats that are experienced with preservation of information through databases are made more exquisite and different with each threat being as complicated as one can think of securing (Andrew Lee, 2005). To effectively manage information in a higher learning institution's context involves the process of applying information security to ensure risks, finances and efforts are balanced while at the same time continuous learning and improvements are cultured (Gefen , 2004). Security should be the concern of everyone in the organization and it should be a way of life within the institution's fraternity.

The Catholic University of Eastern Africa is among the growing number of institutions with growing amounts of delicate data. Interconnectivity of the university with students, lecturer, contractors and even competitors is increasingly required in order to remain competitive and function in the global economy, but every connection adds to the vulnerability of system hackers, criminals, destruction of information by viruses and malware and misuse or destruction of valuable information assets by insiders.

2. UNIVERSITIES' RELIANCE ON INFORMATION SYSTEMS

Universities have adopted information systems and the related technologies so as to gain a competitive edge. In this era effective control of operations and strong strategies are associated with management of quality information. The aspect of readily available information means that universities are affected by their dependence on information and technology resources, systems and the underlying structures that form the basis for this technologies and systems. In universities, reliance on information systems is evident on activities related to creating, using and sharing of information in teaching, learning, research and development and when marketing the university through its websites. It's evident that the amount of intellectual property generated by universities and importance of university information is extensive. The demand for effective information security management is ultimately a combination of various related factors. These factors comprise of reliance of information, increase in the threats that hinder the information that is relied upon heavily and the need for the controls to reduce this ever emerging new risks. Currently there is limited published academic literature that emphasizes on information security management in higher learning. Most of the literature that the study has analyzed so far focuses on information security management in organizations and not universities.

3. STATEMENT OF THE PROBLEM

The adoption of Information Systems (IS) in many businesses is at a fast tempo in order to gain a competitive advantage (Azah N. & Norizan Y. 2010). Universities are relying very much on their information capital and this information is currently facing increasing security vulnerabilities. Reason for this increment is attributed to better use of detection tools by various organizations but still serious challenges are being faced in information systems security management by various institutions. The Catholic University of Eastern Africa is one of the higher learning institutions that is facing security vulnerabilities. In the Past four years, the University has experienced many cases of security breaches, like hacking into the AMS, where student hack into the system and alter their grades, register units they have not yet covered and even grade them. Hacking into the accounting System is another common challenge, where students gain unauthorized access to the accounting system and alter/clear their financial balances. The mailing system of the university has also been facing the unprecedented challenge of hacking, where unauthorized users access the mailing system and use it to send anonymous e-mails to the University management board. Another challenge that the university is facing is unauthorized use of systems at work by employees with vested interests, for example Non-work related upload/download, transmission of confidential data, and unauthorized use of internet in general. Traditional mainstream ISS management research is poorly equipped to identify such challenges much less describe and address them. Thus the study sought to examine the major challenges facing information system security management in higher learning institutions and to find out the improvements that can be done to minimize those challenges.

4. GENERAL OBJECTIVES

The general objective of this study was to understand the major challenges facing Information Systems Security management in institutions of higher learning.

(i) To understand the major challenges facing Information Systems Security management.
(ii) To establish the extent of the use of Information Systems Security Management in higher learning institutions
(iii) To determine if there is any significant relationship between these challenges and information systems security management
(iv) To recommend improvements that can be done to minimize the challenges facing information system security management.

5. SCOPE OF THE STUDY

This study sought to examine the major challenges facing information systems security management in higher learning institutions. Geographically, the study targeted the Catholic university of eastern Africa Main Campus; the management of the university were part of the sample as they were expected to contribute towards answering the questionnaires.

6. LITERATURE REVIEW

Literature related to the study was reviewed in order to gain some insights related to the research problem. Literature in information system security management and challenges facing information system security management was reviewed theories in the relevant field were reviewed and criticized. The theories covered are Security policy theory, Risk management theory and Control and auditing theory

6.1 Conceptual framework

This study was based on the concept that Information system security management depends upon various factors (independent variables). The study conceptualizes two major variables, namely independent variables and dependent variables.

6.2 **Knowledge Gap**

The existing literature on the challenges facing information systems security management focuses on the needs of large corporations that have thousands of employees, complex security needs and large computer systems (Adamkiewicz, 2005). The literature on the challenges facing information systems security management in higher learning institutions is very limited. The literature gap may be due to the evolution of new challenges which initially targeted the computer systems of large corporations and government organizations.

7. METHODOLOGY

This study used descriptive research design. The study aimed at collecting information from respondents on their opinion in relation to the challenges facing information systems security management in higher learning institutions. The research used both qualitative and quantitative research methods. The respondents for this research were drawn from the top management and various departments in the main campus. The sample of this study consisted of 30% of all the members of departments that use the AMS (102) in the Catholic University of Eastern Africa, that is 31 (n=31). A total of thirty one members were selected to respond to the questionnaire. Systematic sampling procedure was used to select thirty percent of the one hundred and two members who use the AMS. Questionnaires were used to collect primary data from the selected sample size. The questionnaires that were used were semi-structured allowing for collection of in-depth information from a relatively large number of respondents as compared to a pure qualitative questionnaire.

8. DATA ANALYSIS AND PRESENTATION

The collected data was analyzed using both quantitative and qualitative data analysis approaches. Quantitative approach involved both descriptive and inferential analysis. Descriptive analysis such as frequencies and percentages were used to present quantitative data summarized in tables based on the major research questions. Data from the questionnaires were checked for completeness, coded and logged into the computer system using Statistical Package for Social Science (SPSS), and the findings recorded and summarized. Pearson's chi square statistic test was used to test whether a significant relationship existed between the challenges and the information systems security management. The conclusions were based on the set decision rule of the probability *(P)* value set at 0.05 level of significance and data was presented in the form of frequency tables.

8.1 Role/position of respondents in university

The study sought for the role of respondents in order to find out the representation of employment categories in the study. A question was posed to all respondents to indicate their role. Data obtained from the field regarding employees' role were analyzed and presented.

Distribution of respondents by their roles

Role	Frequency	Percent
Administrator or Top Management	4	12.9
Head of Section	2	6.5
Middle level staff	23	74.2
Not Indicated	2	6.5
Total	**31**	**100.0**

Source: Survey results, 2012

It is revealed that all the employees that participated in the study held certain position in the institution. The majority, 74.2% were middle level staff, the positions were held by administrator or top management, 12.9% while 6.5% were head of sections. Information on roles was deemed important because these employees were directly involved with information systems in one way or the other hence were well placed to give relevant information on information system security.

8.2 Challenges Facing Information System Security Management

The study sought to explore the challenges facing information system security management in higher institutions of learning – universities. The respondents were asked to respond to indicate on how strongly they agreed or disagreed to the items. The scale was anchored from 1=strongly disagree to 5= strongly agree. The results indicating the number of respondents and the percentage of respondents were as presented in the table. The numbers in parentheses are the % of the respondents. The result suggests that respondents were aware of the challenges facing information system security management in higher institutions of learning though they had mixed reactions towards the challenges. On the strongly agree scale the highest scores were from the items "natural disaster" (n=6, 19.4%), followed by "limited budgets" (n=6, 16.1%) and "outsider access abuse" and "fraud" (n=4, 12.9%) respectively. On the other hand, majority of the respondents tended to disagree with most of the challenge items that were listed. For example, on the strongly disagree scale the highest scores were "fraud" (n=14, 45.2%), and "insider access abuse", "limited budgets"

(n=13, 41.9%) and "integrity" (n=12, 38.7%). The mean and standard deviation of the items about challenges of ISSM in higher institutions of learning were as indicated in the table. The items anchored between 1 to 5, where1=strongly disagree and 5=strongly agree. A mean score on the scale above 3 would indicate that the respondents agree with the statement on the scale, while scores below 2.5 would indicate that the respondents disagree with the statement. From above table the overall mean response rate on the challenges facing information system security management in higher institutions of learning is 2.43 which depicts that the respondents somewhat agree with most of the statements on the scale. For example, the major challenges that institutions of higher learning seem to be faced with are natural disasters (M= 3.06, SD= 1.289), piracy of intellectual property (M=2.77, SD=1.230904), outsider access abuse (M = 2.71, SD = 1.346), cyber theft (M = 2.68, SD = 1.275) and software piracy (M=2.68, SD=1.137). However, insider access abuse (M=1.90, SD=0.978) have little significant as a threat to higher institutions of learning. These findings are similar to Eloff &Solms (2000) who said that information system security is facing unprecedented challenges for example threat of unauthorized users on the internet. Other challenges that the respondents highlighted include: lack of disaster recovery procedure/plan, lack of proper implementation of systems and user acceptability of systems, lack of qualified staff to manage systems and lack of backups and adequate technology to ensure integrity, confidentiality and authentication of data.

8.3 Factor Analysis on the challenges facing information system security management in higher institutions of learning: Factor Analysis: Data reduction technique

In factor analysis there are a lot of items that should be considered in each main construct. Hence, this study employed factor analysis to reduce numerous items. Fourteen (14) items were reduced into four (4) dominant factors. Field (2005) argues that since eigen values measure the substantive importance of a variable, only factors with higher eigen values are retained hence, this study used variables with eigen values greater or equal to 1.00 that were extracted. This section therefore provides summary results of factor analysis. Principle component and varimax rotation techniques were used to run the data reduction. The extracted items were then subjected to further analysis to establish whether they have any significant effect or impact on the way higher institutions of learning manage the information system security. The data reduction analysis is as presented in Table 4.5. Table above lists the eigenvalues associated with each linear factor before extraction, after extraction and after rotation. Before extraction there are 14 linear components identified within the data set. It is clear that there are four (4) factors with eigenvalues greater than 1. The percentage of the variance for these values is explained in column two labeled extraction of sums of squared loadings. While in the third column (rotation sum of squared loadings) the eigenvalues of the factors after rotation are displayed. From the table we can see that factor 1 accounted for considerable more variance (36.890%) than the remaining three. However, after extraction it accounts for 25.342% of variance. Factor loading results in table above indicates that there are four factors (challenges) with highest eigen values which are more than 1. These variables are: hacking, piracy of intellectual property, data availability and insider access abuse hence, were interpreted as the major challenge facing higher learning institutions. Further, the challenges were categorized and interpreted as follows: hacking = 0.820, unauthorized access at work = 0.757, cyber theft = 0.752, outsider access abuse = 0.746 and malware = 0.578 (system vulnerability). Piracy of intellectual property = 0.887, limited budgets = 0.814, software piracy = 0.798 and viruses 0.778 were interpreted as (computer crime and abuse). Data availability = 0.930, integrity = 0.869, natural disasters = 0.673 (environmental security). Lastly, factors insider access abuse = 0.719 and fraud = 0.616 were interpreted to mean (financial backing/security). For example, according to Nissenbaum (2005) disgruntled employees can threaten the security and integrity of information systems. A security survey by Deloitte's Annual technology, media and telecommunications in United States (2010), it was found that 32 per cent of respondents surveyed reduced their information security budgets while budgeting for the following year. The study concluded that this may be due to low concern by the management about the University's Information systems security. This finding is not surprising as this could be related to this study that limited budgets by institutions of higher learning in Kenya was among the significant reasons scoring 0.814 – close to eigen value of 1. When the mean responses for the extent of use of security measures employed in the institutions were computed, the mean was 2.85 as indicated in the table implying that most of the measures asked are employed by the universities to a greater extent. In addition, respondents felt that irrespective of the extent of use and management of information security systems, the following are some of the reasons that hinder its fullest use. They are laxity in adopting quality performing/functioning systems, sabotage, inadequacy of good policies put in place on good management of systems and inadequate training of users of systems.

8.4 Tests of relationships between variables

To establish the existing relationship between variables and to answer the objective 3 "Is there any significant relationship between these challenges and information systems security management?" Pearson Chi-square statistical tests was used in this study to test the significant relation of the challenges on system security management. The results from the Chi-square test are as presented herein against 95% confidence level. The decision rule in this case was that, if the test results showed ($p < 0.05$), then it

was concluded that there is a statistically significant relationship while if the test results were (p>0.05), then it would mean there is no significant relationship between the two variables. Chi-square test results (χ^2 = 9.232, p = .056) in the table drawn from results on the table indicate that there was a statistically significant relationship between the challenge an institution experiences and the management of an information system's security. These results concur with Julie Ryan (2001) assertions in the literature who found out that the challenges of information systems security in universities in the modern context are significant. This was further supported by the descriptive data on Table 4.9 which showed that up to 42.9% of employees agreeing that these challenges affect the systems security to a little extent. On contrary, the majority of the respondents 90.5% disagreed that the challenges affect the institutions to a great extent. However, it was concluded that although there was an agreement, chi-square results indicate that indeed a relation exists hence cannot be ignored. Any challenge experienced may in one way or another influence an institutions system security. It was also of interest of the research to establish how institutions of higher learning are responding to the challenges that they face with regard to information system's security. The descriptive results are as shown in the table next. The results suggest that the most significant response used in the institutions of higher learning was "upgrading technology" (M=3.19, SD=1.046). This implies that institutions upgrading technology without training the staff have no effect on the management of an information system's security. The second most significant strategy used was "auditing the systems or system audit" (M=2.77, SD=1.146). This implies that institutions information system security management objectives and strategies are not realized due to lack of effective follow up. Another significant strategy was "developing a security policy" (M=2.61, SD=1.086). This implies that institutions that have policies on systems security serve as mechanism for implementing and managing an information system's security.

8.5 Factor score of strategies employed towards challenges facing ISSM in higher learning institutions

The table below shows that there are two (2) major factors with eigenvalues greater than 1 that enable higher learning institutions respond to challenges facing information system security management.When the challenges are further rotated using factor loading, variable on establishing ways of dealing with risks during implementation of security measures = 0.935 and developing a security policy = 0.841 were outstanding. According to Schultz et al (2001), computer security policy ensures data confidentiality, integrity and availability within information systems. This finding is also supported by Gaunt (2000) who emphasizes installing an organizational IS security policy. These are the main strategies that can aid institutions of higher learning respond to challenges in implementation of information system security management as shown in table below. Hence, these factors were further categorized into two major groups thus: risk management and information system security policy implementation. The above table clearly demonstrates that the majority of students respondents were of the opinion that continuous training of staff on security issues should be taken a step higher. This was followed by introducing off-site backup systems. In conclusion, the study found that according to respondents, training of staff on information security issues and creating off-site back-up systems are some of the new measures and/or improvements that can be put in place to enhance information system security management at institutions of higher learning. At a Finnish university, a study by Kajava and Siponen (1997) discussed IS security awareness. The study listed principles regarding a security awareness program and methods for awareness, though it failed to offer guidance for practitioners regarding planning and implementing the program in practice.

9. SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

The conceptual framework of the study recognized that indeed security challenges in higher learning institutions impact on an information systems security management. However, with good management strategies in place information systems security management is achievable. The study found out that system vulnerability, computer crime and abuse, environmental security and financial backing/security are key challenges institutions of higher learning are experiencing in the management of their information systems. As concerns the extent of use of security measures employed in the institutions, the mean was 2.85 implying that most of the measures asked are employed by the universities to a greater extent. In addition, respondents felt that irrespective of the extent of use and management of information security systems, the following are some of the reasons that hinder its fullest use; laxity in adopting quality performing/functioning systems, sabotage, inadequacy of good policies put in place on good management of systems and inadequate training of users of systems. When tests for whether there exists any significant relationship between the challenges the institutions face and its influence on information systems security management, chi-square test results (χ^2 = 9.232, p = .056) indicated that there was a statistically significant relationship between the challenge an institution experiences and the management of an information system's security. Therefore, these implied that existence of any information security challenge determines management strategies laid down to mitigate them. The majority of respondents were of the opinion that continuous training of staff on security issues should be taken a step higher. This was followed by introducing off-site backup systems. In conclusion, the study found that according to respondents, training of staff on information security issues and creating off-site back-up systems are some of the new measures and improvements that can be

put in place to enhance information system security management at institutions of higher learning.

10. CONCLUSIONS

Based on the findings of this research the following conclusions were made: System vulnerability, computer crime and abuse, environmental security and financial backing/security are the key challenges found to impact most on information system security management in institutions of higher learning. Institutions of higher learning in Kenya have put measures to improve their information systems security. However, laxity in adopting quality performing/functioning systems, sabotage, inadequacy of good policies put in place on good management of systems and inadequate training of users of systems is a major challenge that affects information systems security in higher learning institutions. The study concluded that there was a statistically significant relationship between challenges an institution experiences and the management of an information system's security and continuous training of staff on information systems security issues was inadequate.

11. RECOMMENDATIONS

The research made the following recommendations based on the findings and conclusions of this research: The university management should come up with ways of identifying the challenges or factors that affect information system security and also identify strategic responses. This can be achieved through implementation of new policies and procedures to guide information system security. Institutions of higher learning should develop programs for monitoring and evaluating information systems security in relation to performance indicators. Also benchmark a systems security with other institutions may also help to improve its security. The university should invest heavily in developing their staff through training programmes e.g. seminars, workshops etc. to further develop their skills and abilities on information systems security issues. This may make up for shortfall in insufficient experience and there is need to implement new measures such as off-site system back-up to secure existing information systems.

12. REFERENCES

[1] Adamkiewicz, S. L. (2005). *The correlation between productivity and the use of information security controls in small business.* The George Washington University, United States –District of Columbia

[2] Anand, S. (2008). Information security implications of Sarbanes-Oxley. *Information Systems Journal: A Global Perspective* Vol. 17(2). pp. 70–75.

[3] Azah A. N., and Norizan M.Y. (2010). An Analysis of Information Systems Security Management (ISSM): The Hierarchical Organizations vs. Emergent Organization, *International Journal of Digital Society (IJDS).*, Vol.1(3). pp. 1- 6

[4] Ba, S. and Pavlou, P. A. (2002). *"Evidence of the Effects of Trust Building Technology in Electronic Markets: Price Premiums and Buyer Behavior,"* MIS Quarterly. Vol 31(2). pp. 295 – 315

[5] Bateson, J. (1997). *Essential of Service marketing*: The Dryden Press, Fort Worth, TX. Vol. 19(5). pp. 191-201

[6] Borg, W.R. and Gall M.D. (1989). *Educational Research*. White Plains, New York: Longman.

[7] Broucek, V. and Turner P. (2003). "*A Forensic Computing Perspective on the Need to Improve User Education for Information Security Management,"* in Current Security Management & Ethical Issues of Information Technology. IRM Press, pp.42-49

[8] Camp, L. J. and Lewis, S. (2004). Economics of Information Security, Dordrecht: Kluwer

[9] Chen, E. (1997), "Active X and Java: the nest virus carriers?" Computer Technology Review, pp. 38-41.

[10] COBIT (2007), *COBIT: Control Objectives*, ISACA, Rolling Meadows, IL., Cybercrime, Webster's New Millennium(tm) Dictionary of English, 2006, Preview Edition, (V0l.9:6) *http://dictionary.reference.com/browse/cybercrime*, retrieved March 15, 2012

[11] Drazin, R. and VandeVen, A.H., (1985), "Alternative forms of fit in contingency theory", *Administrative*

[12] Dhillon, G. (2007). *Principles of Information Systems Security: text and cases.* NY: John Wiley & Sons.

[13] Doherty, N. F. and Fulford, H. (2006). *"Aligning the Information Security Policy with the Strategic Information Systems Plan,"* Computers & Security (23:1), pp. 55 – 63

[14] Doherty, N. F. and Fulford, H. (2005). *"Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis,"* Information Resources Management Journal (18:4), pp. 20 – 38

[15] EC, Commission of the European Communities 2007. *Towards a General Policy on the Fight Against Cyber Crime.* Brussels. Vol. 23(5). pp. 267

[16] Eloff, J. H and Solms (2000). *"What makes an effective information security policy?"* Network Security, (20:6), pp. 14-16.

[17] Ernst and young (2010). *Borderless Security:* Global Information Security Survey, Ernst and Young, London.

[18] Field, A. (2005). *Discovering statistics using SPSS*, (2nd Ed.). London: Sage Publishers

[19] Flynn, N.L. (2001). *The E-policy Handbook: Designing and Implementing Effective E-mail, Internet and Software Policies*, American Management Association, New York, NY.

[20] Gaunt N (2000). *Practical approaches to creating a security culture.* International Journal of Medical Informatics 60(2): 151-157.

[21] Gefen, D. (2004). *"What Makes an ERP Implementation Relationship Worthwhile: Linking Trust*

Mechanisms and ERP Usefulness," Journal of Management Information Systems (21:1), pp. 263 – 288.
[22] Gollmann, D. (1999), *Computer Security*, John Wiley & Sons, New York, NY.,
[23] Grabner-Kräuter, S. (2002). *"The Role of Consumers' Trust in Online-Shopping,"* Journal of Business Ethics 39, pp. 43 – 50
[24] Gupta, M., Charturvedi, A.R., Metha, S., Valeri, L. (2001). "The experimental analysis of Information security management issues for online financial services", *ICIS 2000*, pp.667-675
[25] Harris, S. (2010). CISSP Certification passport,(6th ed.). Berkeley (CA): McGraw - Hill.
[26] Information Today Inc. (2005), Information Today: newspaper for users and producers of electronic information services vol. 22(7). http://www.infotoday.com. Retrieved September 27, 2011
[27] Introna, L. (1997). *Management, Information and Power:* A narrative of the involved manager, London: MacMillan
[28] Kabay, M.E. (1996), *The NCSA Guide to Enterprise Security*, McGraw-Hill, New York, NY.
[29] Kajava, J. and Siponen, M.T. (1997). *Effectively Implemented IS security Awareness* – An Example from University Environment. Proceedings of IFIP-TC 11 (Sec'97/WG 11.1), 13th International
[30] Kothari, C.R. (2004). *Research methodology-Methods and Techniques*, 2nd Revised ed. New Age International Ltd publishers New Delhi.
[31] Lax and Stephen, (2000). *Access Denied in the Information Age*. New York: Palgrave. pp. 253Pages, index. ISBN 0-333-92019-8.
[32] Lee, S.M., Luthans, F., Olson, D.L. (1982). "A management science approach to contingency models of organizational structure", *Academy of Management Journal*, Vol. 25 No.3, pp.553-66.
[33] Lili S, Rajendra P and Theodore J, (2006). An Information System Risk Assessment Model under Dempster – Shafer Theory of Belief function. Journal of Management Information System Vol 22, No. 4 pp. 109-142.
[34] Luthans, F. (1976), *Introduction to Management: A Contingency Approach*, McGraw-Hill, New York, NY
[35] Mahnic V.; Zabkar N.: *The Role of Information System Audits in the Improvement of University Information Systems.* In Proc. 6*th* International Conference of European University Information Systems (EUNIS), Poznan, Poland, 2000; pp 101-110.
[36] Martins A and Eloff JHP (2002). *IS security Culture.* Proceedings of IFIP TC-11 17th International Conference on IS security (SEC2002).
[37] Morse, Neil J., "Protecting Against 'Hactivists,'" *Mortgage Banking*, November 2006, Vol 67(1)
[38] Mugenda, O.M. and Mugenda, A.G. (2003). *Research Methods. Quantitative and Qualitative approaches.* Nairobi: Africa Center for Technology Studies Press.
[39] Nachenberg, C. (1997). *"Computer virus – co-evolution",* Communications of the ACM,January pp 46-51.
[40] National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems* (July 2002); pp 8-15
[41] Nissenbaum, H. 2005. *"Where Computer Security Meets National Security,"* Ethics and Information Technology (7:2), pp. 61 – 73.
[42] Owens, L.K. (2002). Introduction to Survey Research Design. *SRL Fall 2002 Seminar Series*.
[43] Paul J. (2011, December 1). Hackers blamed in KU exam row The Daily Nation. Retrieved [Dec 1, 2011] from http://www.nation.co.ke/News/Hackers+blamed+in+KU+exam+row++/-/1056/1282692/-/113wbgaz/-/index.html
[44] Pennington, R.; Wilcox, H. D. and Grover, V. (2004). *"The Role of System Trust in Business-to Consumer Transactions,"* Journal of Management Information Systems (20:3), pp. 197- 226
[45] Reid, R.C., Floyd, S.A. (2001), "Extending the risk analysis model to include market insurance", *Computers & Security*, Vol. 20 No.4, pp.331-9.
[46] Robbins, S.P. (1994), *Management*, 4th ed., Prentice-Hall, Upper Saddle River, NJ.
[47] Simson, G., Gene, S. (1991). *Practical UNIX Security*, O'Reilly & Associates, Sebastopol, CA.,
[48] Siponen, M. T. (2005). *"Analysis of Modern IS Security Development Approaches: Towards the Next Generation of Social and Adaptable ISS Methods,"* Information and Organization (15:4), pp. 339 – 375
[49] Sitaraman, S. and Venkatesan, S. (2006). *"Computer and Network Forensics,"* in Digital Crime andForensic Science in Cyberspace. Kanellis, P.; Kiountouzis, E.; Kolokotronis, N. & Martakos, D. (eds.), Hershey PA: Idea Group, pp. 55 – 74
[50] Straub, D. W. and Welke R. J. (1998). *"Coping with Systems Risk: Security Planning Models for Management Decision Making,"* MIS Quarterly, (22:4), pp. 441-470.
[51] Symantec. (2008). Small and midsized business products. Retrieved September 26, 2011 from http://www.symantec.com/smb/products/indes.jsp.
[52] Tavani, H. 2000. *"Privacy and Security,"* in: Internet Ethics, Langford, D. (ed.) London: McMillan, pp. 65 – 89.
[53] Thomas, Daniel, "Hack Attacks and Spam Set to Increase," *Computing*, October 7, 2004, VNU Business Publications LTD, London.
[54] http://www.computing.co.uk/computing/news/2071100/hack-attacks-spamset-increase, retrieved September 25, 2011.
[55] Trigaux, R., (2000). "A history of Hacking," *St. Petersburg Times*. http://www.sptimes.com/Hackers/history.hacking.html, retrieved September 23, 2011.
[56] Tudor, J.K. (2001), *Information Security Architecture*, CRC Press, Boca Raton, FL.

[57] United States Code, (2008). *Public Printing and Documents: Definitions*. Title 44, Section 3552. Washington, D.C.: United States Code.
[58] Von Solms, B. (2005), "Information Security governance: COBIT or ISO 17799 or both?" *Computer Security*, Vol 24(2), pp.99-104.
[59] Von Solms, R., Van Haar, H., S.H., Caelli, W.J. (1994), "A framework for information security evaluation", *Information & Management*, Vol. 26 No.3, pp.143-53.
[60] Weber, R. (1999), *Information System Control and Audit*, Prentice-Hall, Englewood Cliffs, NJ.,
[61] Wendy, R. 91997), Strategic Management and Information Systems (2nd edition). Great Britain: Belland Brain Ltd
[62] Wright, M. (1999), "Third generation risk management practices", *Computers & Security*, Vol. 1999 No.2, pp.9-12

ANNEXURE

Figure 1

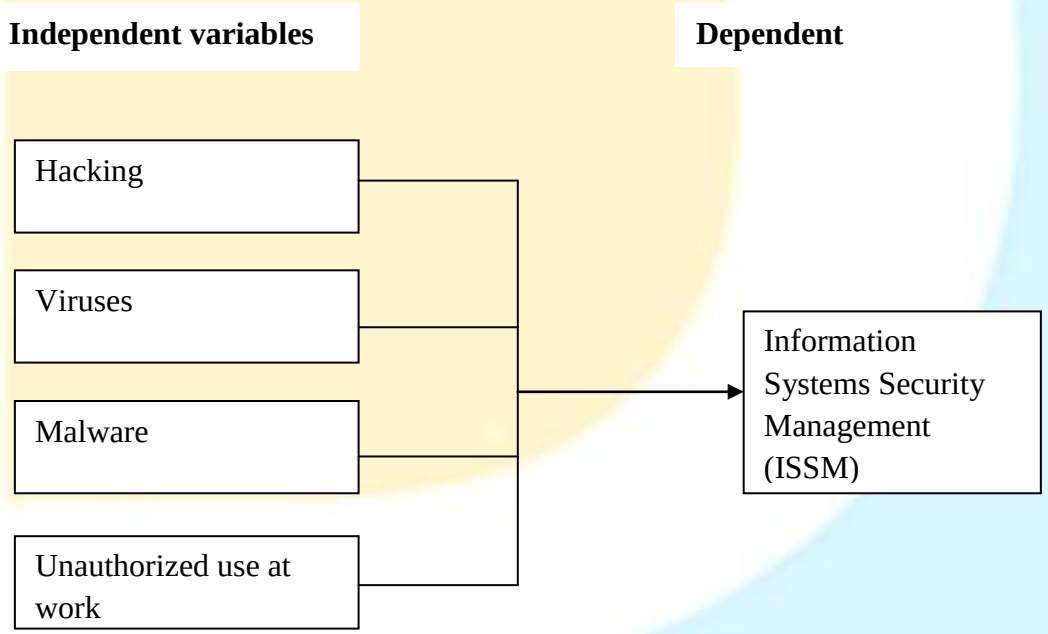

Table 1: Challenges Facing Information System Security Management

	Challenge	Response				
		Strongly Agree	Agree	Neither disagree nor agree	Disagree	Strongly Disagree
a.	Unauthorized access at work	2(6.5)	5(16.1)	3(9.7)	12(38.7)	9(29)
b.	Hacking	2(6.5)	3(9.7)	4(12.9)	13(41.9)	9(29)
c.	Malware	1(3.2)	5(16.1)	8(25.8)	8(25.8)	9(29)
d.	Viruses	1(3.2)	6(19.4)	5(16.1)	12(38.7)	7(22.6)
e.	Cyber theft	3(9.7)	5(16.1)	8(25.8)	10(32.3)	5(16.1)

f.	Fraud	4(12.9)	6(19.4)	3(9.7)	4(12.9)	14(45.2)
g.	Insider access abuse	-	3(9.7)	4(12.9)	11(35.5)	13(41.9)
h.	Data availability	1(3.2)	5(16.1)	2(6.5)	15(48.4)	8(25.8)
i.	Integrity	2(6.5)	4(12.9)	4(12.9)	9(29)	12(38.7)
j.	Outsider access abuse	4(12.9)	6(19.4)	4(12.9)	11(35.5)	6(19.4)
k.	Natural disaster	6(19.4)	5(16.1)	8(25.8)	9(29)	3(9.7)
l.	Software piracy	2(6.5)	6(19.4)	7(22.6)	12(38.7)	4(12.9)
m.	Piracy of intellectual property	3(9.7)	6(19.4)	8(25.8)	9(29)	5(16.1)
n.	Limited budgets	5(16.1)	1(3.2)	1(3.2)	11(35.5)	13(41.9)

Source: Survey results, 2012

Table 2: Overall mean challenges facing information system security management

Challenge	N	Mean	Std. Deviation	Modal Point
5k. Natural disaster	31	3.06	1.289	Agree
5m. Piracy of intellectual property	31	2.77	1.230	Agree
5j. Outsider access abuse	31	2.71	1.346	Agree
5e. Cyber theft	31	2.68	1.275	Agree
5l. Software piracy	31	2.68	1.137	Agree
5d. Viruses	31	2.42	1.148	Disagree
5c. Malware	31	2.35	1.226	Disagree
5f. Fraud	31	2.35	1.624	Disagree
5a. Unauthorized access at work	31	2.32	1.249	Disagree
5b. Hacking	31	2.23	1.175	Disagree
5h. Data availability	31	2.23	1.117	Disagree
5i. Integrity	31	2.19	1.276	Disagree
5n. Limited budgets	31	2.16	1.440	Disagree
5g. Insider access abuse	31	1.90	.978	Disagree
Average		**2.43**	**1.25**	

Source: Survey results, 2012

Table 4: Factor loadings on the challenges facing information system security management in higher institutions of learning: Total Variance Explained

Component	Initial Eigenvalues	Extraction Sums of Squared Loadings	Rotation Sums of Squared Loadings

	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	5.165	36.890	36.890	5.165	36.890	36.890	3.548	25.342	25.342
2	2.288	16.346	53.236	2.288	16.346	53.236	2.891	20.650	45.992
3	1.921	13.720	66.956	1.921	13.720	66.956	2.504	17.884	63.875
4	1.004	7.170	74.125	1.004	7.170	74.125	1.435	10.250	74.125
5	.915	6.537	80.663						
6	.689	4.924	85.587						
7	.454	3.243	88.830						
8	.410	2.932	91.762						
9	.360	2.568	94.330						
10	.257	1.838	96.168						
11	.200	1.428	97.596						
12	.162	1.154	98.750						
13	.100	.713	99.463						
14	.075	.537	100.000						

Extraction Method: Principal Component Analysis.

Source: Survey results, 2012

Table 5: Principle Component analysis of challenges Matrix (a)

	Factor			
Factor	**System vulnerability**	**Computer crime and abuse**	**Environmental security**	**Financial backing**
5b. Hacking	.820			
5a. Unauthorized access at work	.757			
5e. Cyber theft	.752			
5j. Outsider access abuse	.746			
5c. Malware	.578			
5m. Piracy of intellectual property		.887		
5n. Limited budgets		.814		
5l. Software piracy		.798		
5d. Viruses		.778		
5h. Data availability			.930	
5i. Integrity			.869	
5k. Natural disaster			.673	
5g. Insider access abuse				.719
5f. Fraud				.616

Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.

A Rotation converged in 6 iterations.

Source: Survey results, 2012

Table 6: Extent of Use of Information Systems Security Measures in Higher Learning Institutions

Overall mean response rate on extent of use of information systems security measures in higher learning institutions:

Descriptive Statistics

Security Measure	N	Mean	Std. Deviation
6b. Anti-virus	31	3.35	1.330
6f. Authentication	31	3.10	1.326
6g. Anti-phishing	31	3.10	1.326
6l. Backup files	31	3.06	1.389
6k. Email monitoring	31	3.03	1.516
6c. Anti-spy ware	31	2.97	1.140
6o. System controls and audits	31	2.97	1.048
6e. Firewalls	31	2.90	1.446
6h. Network scanners	31	2.84	1.267
6n. Disaster recovery	31	2.81	1.223
6p. Fault tolerant systems	31	2.81	1.195
6i. Intrusion detection software	31	2.68	1.326
6m. Security monitors	31	2.65	1.355
6a. Encryption	31	2.52	.996
6j. Denial of service attack	31	2.52	1.387
6d. Cryptography	31	2.35	1.404
Average		**2.85**	**1.292**

Source: Survey results, 2012

Table 7: Chi-square tests for relationship between challenge and ISSM

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	9.232(a)	4	.056
Likelihood Ratio	9.823	4	.044
N of Valid Cases	31		

a 8 cells (88.9%) have expected count less than 5. The minimum expected count is 58.

Source: Survey results, 2012

Table 8: Contingency table for challenges * ISSM

Challenge		Information System Security Management (ISSM)			Total
		Large Extent	Little Extent	Not at All	
Agree	Count	0	3	4	7

	Expected Count	1.6	4.1	1.4	7.0
	% within challenge	.0%	42.9%	57.1%	100.0%
Disagree	Count	6	13	2	21
	Expected Count	4.7	12.2	4.1	21.0
	% within challenge	28.6%	61.9%	9.5%	100.0%
Neutral	Count	1	2	0	3
	Expected Count	.7	1.7	.6	3.0
	% within challenge	33.3%	66.7%	.0%	100.0%
Total	Count	7	18	6	31
	Expected Count	7.0	18.0	6.0	31.0
	% within challenge	22.6%	58.1%	19.4%	100.0%

Source: Survey results, 2012

Response to challenges facing ISSM in higher learning institutions

Table 9: Descriptive Statistics on strategies employed towards challenges facing ISSM in higher learning institutions

Response	N	Mean	Std. Deviation
7e. Upgrading technology	31	3.19	1.046
7f. Auditing the Academic management system	31	2.77	1.146
7d. Bench marking with other institutions and centers of excellence.	31	2.65	.950
7a. Developing a security policy	31	2.61	1.086
7g. Developing open door policy or open communication with regard to system security issues	31	2.61	1.202
7c. Monitoring and evaluation of the system	31	2.58	1.119
7h. Establishing ways of dealing with risks during implementation of security measures	31	2.58	1.025
7b. Involving an expert to advice on security measures	31	2.45	1.028
7i. Developing a contingency plan	31	2.42	1.119
Average		**2.65**	**1.08**

Source: Survey results, 2012

Table 10: Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %

1	5.682	63.138	63.138	5.682	63.138	63.138	4.045	44.946	44.946
2	1.106	12.287	75.425	1.106	12.287	75.425	2.743	30.479	75.425
3	.631	7.013	82.438						
4	.576	6.401	88.838						
5	.307	3.409	92.248						
6	.285	3.161	95.409						
7	.228	2.537	97.946						
8	.116	1.291	99.237						
9	.069	.763	100.000						

Extraction Method: Principal Component Analysis.

Source: Survey results, 2012

Table 11: Rotated Component Matrix(a) on responses to ISS challenges

Strategy	Factor	
	Risk management	ISS Policy implementation
7h. Establishing ways of dealing with risks during implementation of security measures	.935	
7i. Developing a contingency plan	.868	
7f. Auditing the Academic management system	.818	
7g. Developing open door policy or open communication with regard to system security issues	.740	
7d. Bench marking with other institutions and centers of excellence.	.696	
7e. Upgrading technology	.613	
7a. Developing a security policy		.841
7c. Monitoring and evaluation of the system		.837
7b. Involving an expert to advice on security measures		.728

Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.

Source: Survey results, 2012

Table 12: Improvement measures :Improvement measures of enhancing information system security management (N=31)

Improvement Measure	N
• Continuous training of staff on security issues	**6**
• Introducing off-site backup systems	**2**
• Limit the persons that can access the system at a given time	**1**
• Limit access to sensitive information	**1**

• Audit of systems and implementation of findings	**1**
• Adequate remuneration of employees to avoid corruption cases	**1**
• Proper system implementation plans	**1**
• Employing of security practitioners on full-time basis	**1**
• Advise users to change passwords often	**1**
• Having e-learning materials	**1**
• Implementation of good policies	**1**
• Security standardization	**1**
• Improving network security by closing or disabling network ports e.g. domain ports	**1**

Source: Survey results, 2012