IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 07, Issue 11 (November. 2017), ||VI|| PP 01-06

Effects of Information System Controls on Enhancing Security of Information Systems within Universities: A Case of Public Universities in Western Kenya

OBARA M. A[1], LIYALA S.[2], and OGARA S.[3]
[1,2,3]School of Informatics and Innovative Systems
Jaramogi Oginga Odinga University of Science and Technology

Abstract: Universities in the world today consider information to be their most important asset. They therefore ensure information security by taking appropriate measures to ensure no information is leaked or passed to unauthorized users hence compromising its security. To achieve this, universities should ensure that they have proper infrastructure, policies and standards which are in compliance with the international best practices. The aim of this paperestablished the effect of security controls on information system security implementation in public universities in Western Kenya. The study used the business model for information security. A descriptive survey that targets information security professionals was carried out in four public universities in Western Kenya. The population of the study consisted of ICT directors, network administrators, web administrators, user support technician and computer lab technician in the selected universities. Quantitative data was collected from a sample of thirty-nine information management team within chosen universities, which were purposively selected to form the study size. Descriptive statistics was used for data analysis and results were presented using tables. The study established that cybercrime is on the increase in public universities. The empirical findings from study highlight regular audits on Information security systems should be conducted in public universities to establish whether the security functionalities put in place are working as intended.

Keywords: Information Systems Controls, Information Security, Information Systems, Public Universities

Date of Submission: 23-10-2017 Date of acceptance: 17-11-2017

I. INTRODUCTION

Institutions of higher learning are increasingly using Information and Communication systems in administration, teaching, learning and research. This infrastructure needs to be available, secure and well protected. It therefore becomes crucial for information security practitioners in public universities to implement effective information security programs. Information security focuses on technological issues and important elements of an organization such as people, process, business strategies etc., which also mandates the need for information security. A comprehensive security framework incorporates three basic components: people, technology, and process. When correctly assembled, the people, technology, and process elements of an information security framework work together to secure the environment and remain consistent with an institutions business objectives [1].

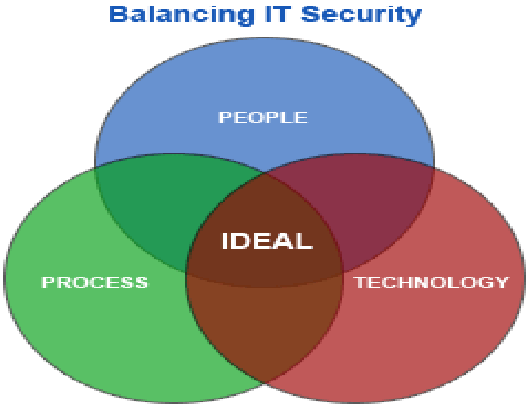

Figure 1: Concept of People, Process and Technology

Attacks upon information security infrastructures have continued to evolve steadily overtime making the management of information security more complex and challenging than ever before [2].

Information security management systems should be implemented, maintained, monitored and reviewed regularly to ensure their effectiveness. This is according to the best practices in information security [3]. Information management System's failure is very critical and would lead to losses for a university. For example, the failure of the integrated Financial Management System could lead to the process of admission of students and recruitment of new staff coming to a standstill as this system crucial. Failure of examination systems that process examination results would have devastating impact on the reputation of the university. The risk levels to the university information systems have increased as the IT adoption increases.

Universities and other institutions of higher learning do not report small- scale hacks as they are afraid of the consequences, this would lead to large-scale damage to their reputation [4]. This can be supported by the infamous New York Times (NYT) and Wall Street Journal (WSJ) attacks. The security company hired by the NYT reckons that the hacking against the NYT went on for several months and that the hackers used university computers, hopping IP addresses to hide the attack source. Accessing the university computers in Wisconsin, New Mexico, Arizona and North Carolina was easy for the Chinese hackers, since university computers are similar to small business computers, in that they do not have massive security operations in place to cover them.

Cyber-attacks have more than doubled over the last year in Kenya to stand at 5.4 million. Releasing the Kenya cyber security report 2014 June, Mr. William Makatiani, the managing director of Serianu Ltd, said the breaches costed an estimated Sh5 billion. Top attacks on Kenyan systems came from Germany and Kenya itself. In 2012, China topped the list. The report argues that cyber-terrorists, spies, hackers and fraudsters are increasingly motivated to target ICT infrastructure due to the increasing value of information held within it, driven by growing dependence on them and the perceived lower risk of detection and capture as compared to more traditional crime. The same report concludes that there is a growing population of people who discover the vulnerabilities in information systems and see ways of making money hence likelihood of more information security threats and bigger losses for organizations like public universities and the economy. This makes it necessary to protect our information systems.

Kenyan universities are among institutions topping a list of hacking targets in Africa after Egypt, Morocco and South Africa [5]. The hackers tamper with the institutions systems to adjust grades and fee balances especially towards the end of semester and during the graduation period. This implies that public universities in Kenyan must prioritize the security of their information systems in order to provide their users with information that is available, accurate and confidential. This is further complicated by foreign state-sponsored actors from countries like China who provide an insider threat to local academic and research institutions, since a common occurrence is the insider threat. Hacktivists from China come into the United States, secure employment at academic and research institutions as professors, or enroll as foreign students, simply to hack the university networks.

Some of the incidents reported by foreign universities includes in 2012, a Florida State University Panama City student hacked the school's Wi-Fi network, and redirected everyone who accessed it to a homosexual pornography website. The students wanted to show the administration that the network was not secure enough, as no password was required for its use. Other university hacking examples include hacking the college systems in order to change grades, rig on-campus elections and cheat on examinations [4]. In February 21st 2014, university of Maryland reported that hackers had gained access to the university server and stolen names, Social Security numbers, birth dates and the university identification numbers of 309,079 people affiliated with campuses at College Park and Shady Grove since 1998. The university said no financial, academic, health or contact information was stolen in the breach [6].

Other examples of cyber-attacks facing institutions of higher learning is a case of ButlerUniversity in Indianapolis, in which databreach affecting 163,000 students, faculty, staff and alumni was experienced [7]. This implies that the potential threat to information systems is not just a current problem but a future problem as well.

II. LITERATURE REVIEW

2.1 Security Controls

Information security controls are the technical, process, physical, and policy safeguards designed to protect sensitive data by mitigating the identified and assessed risks to its confidentiality, integrity, and availability [8]. The management of universities has a responsibility to ensure the integration of security controls through-out the institution governed by organizational policies and practices while enforcing compliance with the security program and ensuring an effective information security awareness program implementation. Controls should not only be internal but external as well. Information security managers are responsible for ensuring the presence and effectiveness of internal controls.

While it is not possible to eliminate all security challenges facing universities, the security controls should integrate and coordinate people, process and technology to establish multiple security countermeasures to protect the confidentiality and integrity of information assets. This can be done using Defense in Depth strategy which is a multilayered defense strategy in which multiple related actions and controls are applied to minimize failures and compromises and their propagation. It is designed on the principle that multiple layers of different types of protection presenting unique obstacles will increase the likelihood of being able to identify and prevent an attack from occurring. Each protection layer has unique characteristics, presenting successive obstacles for an intruder to overcome. Defense in Depth follows a systems approach which integrates people, technology and processes [9].

People-Focuses on senior level management support, assignment of specific roles and responsibilities, resource allocation, personnel training and accountability; Technology-Multiple and layered technological defenses outside, at, and within the perimeter, including encryption, firewalls, intrusion detection, transmission and remote access controls and antivirus and patch management; Processes- The activities required to sustain a university's security on a daily basis, including security policies, risk assessments, security and vulnerability reviews, process controls, and incident response planning.

Some of the considerations universities should address during control selection and implementation include:

- What are the controls necessary to adequately protect institutions information?
- Have these security controls been implemented? If not is there a realistic plan for their implementation?
- What level of assurance is there that the selected controls are effective as implemented?

2.1.1 Types of information security Controls

Many studies have revealed that organizations implement security controls without proper security policies leading to inadequate information security [10]. For effective information system security implementation, controls can be placed in three categories:

- Physical Controls: These are security measures taken by the universities to control physical access to devices and defined structure. Physical controls are an essential step as it protects the physical environment where critical information is stored and processed [11].
- Technical / Access Controls Access controls: These are security features that control how users and systems communicate and interact with other systems and resources [12]. Access control is used to grant permissions to users to access certain information depending on the sensitivity, criticality and confidentaility of the Information [13]. This is done through authentication; a process of identifying the user through his credentials as known by the system such as name, username, password, biometric credentials where a physical characteristic such as a fingerprint or voice or eye scan is used to identify and authenticate an individual. The user identifies himself to the system and the system confirms or authenticates the individual.
- Process Controls: These refer to the policies, procedures, and processes set by the information managers in universities to define and guide user actions and restrictions in dealing with sensitive information. This security policy provides direction for each employee and department regarding how security should be implemented and followed, and the repercussions for noncompliance. Procedures, guidelines, and standards provide the details that support and enforce the organization's security policy.

  Within these major categories, controls can further be defined by what they do, including: Preventive-This control acts to limit the likelihood of a threat by preventing intentional or unintentional unauthorized disclosure of sensitive information; Detective-It detects and report actual or attempted unauthorized events by helping identify harmful actions as they occur; Corrective-It responds to security incidents and terminate harmful events or reduce their damage.

III. METHODOLOGY

This section covers the methodological design used in the study, which was based on the five layers of the research onion [14].The study was carried out among public universities in the western Kenya region comprising of the old Nyanza and Western provinces.Research onion model was used to guide the key components of the research design. This study settled on descriptive design which was found to be more applicable. On the research method, this study used the mono method because it employed the use of one research approach. On the choice of time horizon, this study used cross sectional time horizon because the study was to be carried out within a specific period of time and required data to be collected once. Sectional time horizon was useful in the study because it allows the establishment of some control over the variables being studied. Data was collected using questionnaires and analysed.

The target population for this study was public universities in Kenya. There are 23 publicuniversities in Kenya [15]. It is from this population that a sample was drawn. Respondents for this study included IT professionals working in the public universities and deals with issues pertaining to information security.

Purposive sampling was used and only IT professionals dealing with the information security function of the university were included. Purposive sampling is the rationale for undertaking case study research [16]. From the purposive sample the researcher managed to get 35 respondents who met the requirements threshold of the population in %. Respondents were selected from Maseno University, Jaramogi Oginga Odinga university of Science and Technology, Masinde Muliro University and Kisii University. Survey method was used by the researcher so as to target fewer universities but at the same time get in-depth information from the selected universities. Within the universities simple random sampling was used on IT professionals.

Table 3.1: Participants in the questionnaire

No:	**Title**
~~1.~~	~~Director ICT~~
2.	Network administrator
3.	Web administrator
4.	User support technician
5.	Computer lab technician

The above list comprised of individuals with diverse roles that were deemed adequate and representative of the university operations. The input of the above participants was crucial for this study as they brought a different dimension with regard to the data collected.

The sample size for questionnaire respondents was determined using Yamane's simplified formula [17], which is as follows:

$n= N/ (1+N (e)^{2})$ ……………………………………………………………(Eqn. 1)

Where $e^{2} = 0.05^{2}$and is the confidence level

n is the desired sample size

N is the total population under study

When the formula (Eqn. 1) was applied to the 39 potential respondents, it yielded a sample size of 35. The sample size of the members of staff was distributed among the various departments using proportionate sampling. Stratified Simple random sampling was used to select items from each stratum using the list of members in the ICT department.

Therefore, the table below shows the summary of the sample population and the sample size.

Table 3.2: Sample Population and Sample Size

	UNIVERSITY	DEPARTMENT	POPULATION	SAMPLE SIZE
	Jaramogi Oginga Odinga University of Science and Technology	Director ICT services department	1	1
		Network Administrator	1	1
		Web Administrator	1	1
		User Support technician	1	1
		Computer lab technicians	4	3
	Kisii University	Director ICT services department	1	1
		Network Administrator	1	1
		Web Administrator	1	1
		User Support technician	2	2
		Computer lab technicians	3	3
	Maseno University	Director ICT services department	1	1
		Network Administrator	3	2
		Web Administrator	2	2
		User Support technician	3	2
		Computer lab technicians	8	7
	Masinde Muliro University	Director ICT services department	1	1
		Network Administrator	1	1
		Web Administrator	0	0
		User Support technician	2	2
		Computer lab technicians	2	2
		Total	39	35

This study used both primary and secondary data. Questionnaires were used to collect primary data. Questionnaires when used in survey is less costly, can be used in widely spread geographically areas, is free from bias and gives the respondents time to give well thought of answers [18]. The questionnaires contained open and closed ended questions and was divided into two sections, A and B. Section A focused on the profile of the respondents while section B contained questions on the research objectives. Secondary data was gathered from organization reports, publications and other literature relating to the implementation of system security frameworks in public universities in Kenyan.

The study used questionnaires based on the objectives and certain general questions touching on security implementation. This was then pre tested in one of the public universities that were not part of the sample.

The results from the questionnaires were then prepared for entry, coding and later for analysis using the various data analysis procedures before being presented.Data analysis was done using descriptive analysis of the questionnaires. Other statistical tools that were used are charts, tables and frequency analysis. This study generated quantitative data. Completed questionnaires were checked, coded and entered in to an excel database. Data was analyzed using regression to get frequencies, percentages and cumulative percentages which were tabulated and presented in pie charts and graphs. Regression analysis was also be used to find the relationship between the dependent variable and the independent variables.

IV. RESULTS AND DISCUSSIONS

The opinion of the respondents were sought on security measures being implemented by public universities to curb cyber-crime. The study findings in table 4.1 indicates the dependent variable (secure system) is strongly positively correlated to Centralized Backup with r =0.822, Network firewall r = 0.789, Intrusion prevention system r = 0.796, Secure Sockets Layer r =0.822, Encryption r = 0.516, VPN for remote access r = 0.857, Active Content Monitoring, r = 0.820, (p<0.05 in all cases).

Table 4.1: Correlation between security controls and secure system

Correlations

		Secure system	Centralized Backup	Network firewall	Intrusion prevention system	Intrusion Detection system	Secure Sockets Layer	Encrypt	VPN for remote access	Active Content Monitoring
Pearson Correlation	Secure system	1.000	0.822	0.789	0.796	0.816	0.822	0.516	0.857	0.820
Sig. (1-tailed)	Secure system	.	0.000	0.000	0.000	0.000	0.000	0.002	0.000	0.000

The results in table 4.2 indicates that security controls implemented explained 84% (R^2=0.84) of the variance in a secure information system. While 16% is due to circumstances beyond the researcher's control. The results also show a strong positive relationship between security controls and a secure information system(R=0.92). The Durbin-Watson coefficient is close to 2, indicating few negative autocorrelations.

Table 4.2: *Model Output: Security Controls*

Model Output	
Multiple R	0.912
R Square	0.839
Adjusted R Square	0.785
Standard Error	0.272
Durbin Watson	1.791

Table 4.3 indicates that the model from the security controls was adequate to explain the dependent variable (secure systems) with F-value (7,21) =15.631, p<0.05 is significant hence security controls can be used to model the responses for dependent variable.

Table 4.3: *ANOVA: Security Controls (Research data; 2015)*

ANOVA

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	8.115	7	1.159	15.631	P<0.05
	Residual	1.557	21	.074		

Total	9.672	28

V. CONCLUSIONS

The main objective of this study was to determine the effect of information system security controls on information system security implementation within public universities in Western Kenya. Based on questionnaire data, there was a positive effect of information system security controls on secure information system implementation in universities in western Kenya. Data analysed indicated that R is 0.92 and R^2 is 0.84, implying a strong positive relationship between information system security controls and secure information system. Hence, security controls had a strong positive effect on secure information system. Challenges identified in implementing security controls included; lack of resources, in adequate senior management support, risk assessment not being carried out regularly and inappropriate infrastructure. The mitigation measures to the challenges included; resource provision, support from management, regular risk assessment to ensure the control measures are working and appropriate infrastructure to cope with the ever increasing challenges. This research provides more opportunities in the extension of the scope of study to cover other public universities in Kenya. This comparative findings shall hasten the significant contribution of information system security controls on information system security implementation.

REFERENCES

[1]. Khalid K, Paul S, Jonathan P, Laura K & Jennifer A.Defining A High- Level Security Framework. Putting Basic Security Principles To Work (2007)

[2]. Deloitte East Africa. East Africa Application Security Survey, safeguarding the future [online]. Retrieved February 2015 from http://www.deloitte.com/view/en_KE/ke/eamedia/kepublications/surveyreports/index.htm.

[3]. Arnason, S.T. and Willet, K.D. How to Achieve 27001 Certification: An Example of Applied Compliance Management. New York: Auerbach Publications. 2008.

[4]. Rasmussen Rod. The College Cyber Security Tightrope: Higher Education Institutions FaceGreater Risks. Retrieved 3rd March 2016 from http://www.securityweek.com/college-cyber-security-tightrope-higher-education .

[5]. Letoo Stephen, The star newspaper, “Kenya universities top list of hacker targets in Africa” 4th August 2015

[6]. Bob Niedt.Washington Business Journal. 2014 21st February

[7]. Jeffrey Roman. Latest Incident Highlights Breach Vulnerabilities in Academia. June 2014

[8]. Elsevier.**Controls-and-Safeguards.pdf** retrieved on 3rd May 2015 from http://www.scitechconnect.elsevier.com/wp.../

[9]. Garcia, M. L. The design and evaluation of physical protection systems. Boston: Butterworth-Heinemann. 2001.

[10]. Doherty F. N. The information security policy unpacked; A critical study of the content of university policies. 2011.

[11]. Hughes, Alan. Information security procedures. Retrieved 4th April 2014 from http://www.ehow.com/way_5676002_Information-security-procedures.html

[12]. Easttom W. C. Computer Security Fundamentals, 2nd ed.2011.

[13]. Tipton, Harold F. and Micki K. eds. Information Security Management Handbook, 4th Edition. New York: Auerbach Publications. 2000.

[14]. Saunders,M.,Lewis,P.,&Thonhill,A.Research Methods for Business students, (5th edition). London: Pearson. 2009.

[15]. Commission of University Education.www.cue.or.ke (2015)

[16]. Creswell, W. Research Design: Qualitative, Quantitative and Mixed Methods Approaches. (2nded). London: Sage publications Inc. 2003.

[17]. Israel, G. Determining Sample Size. IFAS Extension: University of Florida. Retrieved on 23rd June 2015. http://edis.ifas.ufl.edu.

[18]. Kothari, C.R. Research Methodology- Methods and Techniques, 2nd Revised Edition. New Delhi: New Age International (P) Limited Publishers. 2004.

OBARA M. A Effects of Information System Controls on Enhancing Security of Information Systems within Universities: A Case of Public Universities in Western Kenya IOSR Journal of Engineering (IOSRJEN) 07.11 (2017): 01-06.