Mbabazi, 3(11): November 2016] ISSN 2348 – 8034
DOI- 10.5281/zenodo.165718 Impact Factor- 4.022

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

ASSESSING THE IMPLEMENTATION OF INFORMATION SECURITY POLICY IN UGANDAN UNIVERSITIES

Businge Phelix Mbabazi[*1], Kareyo Margaret[2] and JWF Muwanga–Zake[3]

[*1]PhD Candidate –Management Information Systems, Kampala International University,
[2]Dean, School of Computing and Information Technology, Kampala International University,
[3]Senior Lecturer, School of Computing and Information Technology, Kampala International University

ABSTRACT

Information security program endeavors to ensure that the organization's information and its processing resources are available when authorized users need them. Universities which are vulnerable have formulated Information security policy, which among things address security concerns. Such institutions make use of Encryption System. Encrypting such files at least helps protect institutions with physical security policy, digital rights management systems which prevent unauthorized use.The study aimed at assessing the implementation level of information security policy in universities in Uganda and recommend on the areas where they are not being implemented. The population of study comprised 164 staff members from seven Universities. Findings showed on average most of the policies were being implemented like policy on Access control, policy on acceptable use of workstations in their Institutional and policy on acceptable use of wireless devices except policy on Bring Your Own Device to be used at the Institution and Data destruction policy among others which were partly implemented

Keywords:- *Information security, Universities, policy*

I. INTRODUCTION

The Uganda Internet Governance Forum report (2012) shows that Uganda has made progress on implementing some key Internet Governance issues. Internet Governance focuses included affordability and access to cyber security management and critical Internet resources. On cyber security management, Uganda has operationalised cyber laws, including the Computer Misuse Act (2010), Electronic transactions Act (2011) and the Electronic Signatures Act, 2011. The ICT ministry has developed the Information Technology Policy (2012) and NITA-U has also come up with the National Information Security policy (2014), all these have come up in order to create awareness information security awareness in order to mitigate the risk of information insecurity in organizations. However, a major problem is that the success rates of the implementation of the security policies are not known, particularly in Higher Education (HE) institutions in Uganda

1.1 Security of Information in Organizations

Significant research has been carried out about information security-related behavior in institutions. For example, it has been established that work threats can be divided into two: those external to an institution and those internal to an institution. The two divisions are argued on the basis of the likelihood that threats often trunk from diverse motivations. It appears, however, that higher education institutions tend to ignore insider threats and therefore, that insider threats are less researched. Insider threats include human versus non-human and accidental versus intentional (Loch et al. 1992).

It is assumed that policies that higher education management sets and implements to protect the information systems assets are headed by the employees. Policies are used to present expected behavior of employees when using enterprise assets and what noncompliance can lead to. There is nonetheless an element of trust between management and employees, since management expects employees to work efficiently. According to Peltier (2005), an effective information security program endeavors to ensure that the organization's information and its processing resources are available when authorized users need them.

Bogere, Haolader, and Mahbubur (2013) observe that Academic Institutions in Uganda which are vulnerable have formulated ICT policies, inter alia address security concerns. For example, institutions make use of Encryption System. Encrypting files at least help protect institutions with physical security policy, digital rights management systems which prevent unauthorized use. Additionally, Access Control Systems (ACS) are used to control access to information and computer systems. The aim of the ACS is to define a set of account

Mbabazi, 3(11): November 2016] ISSN 2348 – 8034
DOI- 10.5281/zenodo.165718 Impact Factor- 4.022

management standards that will restrict access to authorized personnel and safeguard the services and information. This is done mostly by use of passwords. HE in Uganda has unfortunately, apparently, not cared to study and other security systems, and to set policies concomitant with the chosen security systems. Many Ugandan higher education institutions are yet to determine the best ways to adopt security policies.

Hence, many challenges face higher education in Uganda, not least understanding the insider threats, and to what extent security policies are implemented. This paper presents a study carried out in a number of Ugandan HE institutions that aimed at assessing the implementation level of information security policy in universities in Uganda.

1.2 Information Security in Uganda

The National ICT policy of Uganda (2012) argues that, the rising tendency for improved information access/exchange resulting from integrating ICTs within the social, cultural and economic field of a country can also bring in number of security, privacy and consumer safeguard concerns that need to be addressed as part of the efforts of developing an information society.

Uganda like most countries in the world is susceptible to some of the negative implications that may hinder the mainstreaming of ICTs in society. Therefore, definite safety measures and mechanisms to ensure the safety of people, communities, businesses and the nation at large are needed as part of implementing this policy. The National ICT policy of Uganda, (2012) highlights among others the following.

1. Securing the nation's electronic communication system both for individual, private and public as part of creating the information society;
2. Enhancing user confidence and trust among the public as well as to both protect data and network integrity;
3. Preventing, detecting and responding to cybercrime and abuse of ICT so as to contribute to the fight against national, regional and international crimes such as pornography, fraud, money laundering, drug trafficking and terrorism;
4. Implementing ICT Security awareness programmes amongst users and the public;
5. Implementing systems that will help in the discovery, avoidance and timely response to threats relating to ICT crimes and misuse;

There was a widespread belief among Ugandans that exposure of students to computers would increase their educational achievement and greatly enhanced their employability after school. In fact various technocrats are of the view that integration of ICT into their world of work will improve their own performance and commitment. This has led rapid increase in the use of ICTs in Universities which now calls for security controls to maintain the technology introduced (Bogere et al. 2013). Therefore, Bogere et al. (2013) recommends that ICT security should be included in university budget, so that it would help in allocating a specific amount of the university funds to maintain ICT security within the university. They additionally advise that formalized ICT security policies should be designed to govern all loop holes within the ICT security system of a university

According to National Information Security Policy (2014), an information security policy helps improve security if published, enforced, audited and updated to reflect organizational requirements among others that :

1. All institutions using portable and removable media must adopt official measures to avoid the unauthorized disclosure, alteration, deletion or damage of assets, and interruption to business activities
2. All institutions must adopt official policies and measures to backup and regularly test copies of information and software required to recover from major disruptions
3. Institutions should make certain that users know their information security everyday jobs in order to reduce the risk of theft, fraud or misuse of facilities
4. All institutions should perform Baseline Security checks to ensure that the character and personal circumstances of individuals seeking employment before being entrusted with access to critical infrastructure and after being employed.
5. All Institutions should implement suitable security procedures to mitigate remote access risks
6. All institutions should have appropriate physical security perimeters to shield facilities hosting critical infrastructure against a range of physical security threats including crime, natural disasters and acts of terrorism
7. All institutions should adopt formal measures to enable the secure discarding and re-use of storage media

Mbabazi, 3(11): November 2016]
DOI- 10.5281/zenodo.165718

ISSN 2348 – 8034
Impact Factor- 4.022

According to National Information Security Strategy ,(2011) The ICT Sector has been overtaken by various security emerging threats such as; advanced identity thefts, increasingly sophisticated cyber attacks, botnets, social engineering, cyber espionage ,mobile phone and VoIP threats, increasingly malicious web application vulnerability exploits, and supply chain attacks infecting consumer devices distributed by trusted organizations. The following table shows the Analysis of Information Security soft controls among Ugandan Government Organizations and Information security maturity in Uganda.

Information Security Control	in place	not in
Test environment for applications testing before moving to live environment	27%	73%
Quality Assurance /IT Audit on the organizational environment	36%	64%
Review and updating IT Security Policy	55%	45%
Developing and rolling out a security awareness program	36%	64%
Drafting IT Security incident management procedures	36%	64%
Review and update change management policies and procedures	36%	64%
Scanning of the network and identifying and closing ports open but not in use	64%	36%
Review Telnet and FTP usage and seek secure options	64%	36%
Security updates and alerts knowledge management	40%	60%
Password and access control procedures hardening and enforcing	82%	18%
The presention of these results show that there are still major challenges in implenting soft controls.		

Figure 1.1: Analysis of Information Security soft controls (Source: NISS, 2011)

Information security maturity in Uganda

This figure clearly shows the areas of weakness in Uganda as far as Information Security is concerned. (NISS, 2011)

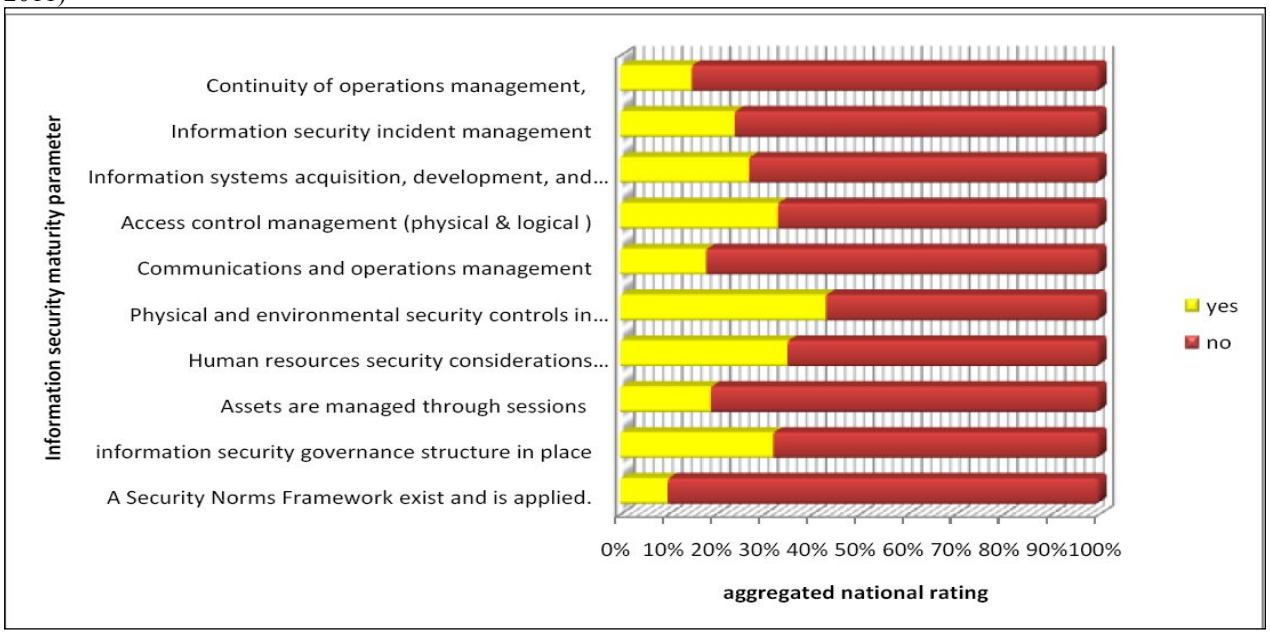

Figure 1.2: Information Security Maturity in Uganda (Source:NISS, 2011)

Mbabazi, 3(11): November 2016] ISSN 2348 – 8034
DOI- 10.5281/zenodo.165718 Impact Factor- 4.022

The figure above showed that information security maturity parameters were below 50% for example information security governance structure in place was only agreed by 35%; a security norms framework exits and is applied only 10 % agrees that they are applied and exits and only 30% agreed that there are access control management (physical and logical) while physical and environmental security controls had 45% of respondents agreed that they exit.

1.3 Information Security Policy in Universities

The purpose of information security is to protect an organisation's valuable resources, such as information, hardware, and software. Through the selection and application of appropriate safeguards, security helps the organisation's mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets. Unfortunately, security is sometimes viewed as thwarting the mission of the organization by imposing poorly selected, bothersome rules and procedures on users, managers, and systems. On the contrary, well-chosen security rules and procedures do not exist for their own sake, they are put in place to protect important assets and thereby support the overall organizational mission (Bogere et al, 2013).

According to Ndejje University IT Services (NIS) Laboratory Security Policy (2008), the policy covers any method of information creation or collection, including electronic capture and storage, manual paper records, video and audio recordings and any images, however created. The Policy however is for all Laboratory clients including the students and Staff who use the facility to study, teach and access other materials. They include software security, hardware security, system security and physical security.

George Washington University (2014) suggests that Information Security policy is to maintain the privacy, truthfulness, accessibility and regulatory compliance of Non-Public Information stored, processed and/or transmitted at the university is a requirement of all legitimate users.

According to the George Washington University (2014) the following necessities are appropriate to all legitimate users with access to Non-Public Information:

a) Notifying their suitable university official and the IT Support Center immediately in case of data breach or other system access control mechanisms are lost, stolen or disclosed or suspected of being lost, stolen or disclosed.
b) Restricting physical access to laptop computers when you are physically away from your office or work space, by, for example, locking the door or using security cables or locking devices.
c) Securing your mobile device using a screen saver or built-in lock feature whenever you are not using it.
d) Maintaining control of your mobile devices to reduce the risk of theft and unauthorized access.
e) Securing computers and mobile devices by requiring passwords
f) Logging out whenever you have finished using the information system.
g) Use secure methods in transmitting Non-Public Information.

According to University of Bristol (2014) Information is a vital asset to any institution and this is especially so in a knowledge-driven institution such as the University of Bristol, where information relate to learning and teaching, research, administration and management. The policy is concerned with the management and security of the University's information assets and the use made of these assets by its members and others who may legitimately process University information on behalf of the University. The University policy comprises of Business Continuity, Compliance, Outsourcing and Third Party Compliance, Operations, Information Handling, User Management, Acceptable Use, Network Management, Software Management, Mobile and Remote Working, Encryption among others.

University of Leicester (2011) University relies on computer systems and, to a lesser extent, manual procedures for handling and processing the information supporting many of its activities. Information that the University manages shall be appropriately secured to protect against consequences of breaches of confidentiality, failures of integrity, interruption to availability and failure to comply with legal requirements. (The University must comply with relevant statutory or other overriding requirements affecting information security, whether or not they are explicitly stated within its policies)

II. METHODOLOGY

This study targeted a population of 450 comprising of Heads of Department and ICT Technical Staff member selected from (2) public degree awarding Institutions namely; Mbarara University of Science and Technology, Muni University and seven(7) private Universities namely Kampala International University, Cavendish

University, International University of East Africa, , St Augustine University, Mutesa 1 Royal University ,Islamic University in Uganda and Ndejje University, from January 2014-August 2015.

The minimum sample size of 212 was computed using the Sloven's formula given by;
$n=N/(1+N*e^2)$ Where; n = sample size; N = Population size and e = level of significance / error (0.05)
The researcher used questionnaire to collect data from the respondents. Questionnaires was used because the sample size was large enough thus they provide the advantage of being more reliable and applicable under survey design. The method was also preferred for its merits as advanced by (Gillham, 2000), which include management of resources, distance, cost and time. In this situation the measurement of constructs in this case therefore was done using Likert's measuring scale and thus the levels of the constructs were estimated basing on the response modes and scoring system of a rage of five(5).

The data was collected through a structured questionnaire and was coded and entered into the computer system and statistically treated using the special package for social scientists (SPSS).frequencies and percentage distributions were used to analyze data on the respondent's profile and the results were presented in form of tables.

III. RESULTS & DISCUSSION

A total of 164 responded in answering the implementation level of information security policies in institutions with 128 respondents representing private universities while 36 respondents represented the public universities in Uganda.

Implementation of Information security policy in Universities

	Information security policy	***Sample Size***	***Mean***	***Std. Deviation***	***coefficient of variation***	***Interpretation***
1.	Policy on Bring Your Own Device to be used at the Institution	164	3.0	1.228	40.93	Partially Implemented
2.	Data destruction policy	164	3.4	1.195	35.15	Partially Implemented
3.	Policy on regular review of the different information security policies	164	3.4	1.154	33.94	Partially Implemented
4.	Policy on response of Information Systems security events	164	3.4	1.167	34.32	Partially Implemented
5.	Policy on reporting of Information Systems security events	164	3.5	1.240	35.43	Implemented
6.	Offsite storage Policy	164	3.5	1.398	39.94	Implemented
7.	Policy on cyber security	164	3.5	1.354	38.69	Implemented
8.	Data retention Policy	164	3.6	1.177	32.69	Implemented
9.	Policy on sharing of Institutional data via the network	164	3.6	1.378	38.28	Implemented
10.	Data classification Policy	164	3.6	1.080	30.00	Implemented
11.	Policy on storing of Institutional data via network	164	3.7	1.303	35.22	Implemented
12.	Policy on access control	164	3.7	1.318	35.62	Implemented
13.	Policy on acceptable use of workstations in your Institutional	164	3.7	1.310	35.41	Implemented
14.	Back-ups storage Policy	164	3.7	1.317	35.59	Implemented
15.	Policy on acceptable use of wireless devices	164	3.8	1.228	32.32	Implemented

16.	Policy on acceptable use of e-mails in your Institutional	164	3.9	1.223	31.36	Implemented
Mean		**164**	**3.58**	**1.250**	**35.03**	**Implemented**

Source: Primary Data 2015

According to the Table above, the results showed that majority of the information security policies were being implemented namely; policy on reporting of Information Systems security events, offsite storage policy; policy on cyber security; data retention policy; policy on sharing of Institutional data via the network; data classification policy; policy on storing of Institutional data via network; policy on access control, policy on acceptable use of workstations in your institutional; Backups storage policy, policy on acceptable use of wireless devices; policy on acceptable use of e-mails in your Institutional. However some policies were partially implemented and these included; Policy on Bring Your Own Device to be used at the Institution as far as Institutional data security (Mean=3.0, coefficient of variation =40.93 and Std deviation=1.228); data destruction policies (Mean=3.4, coefficient of variation =35.15 and Std deviation=1.195); Policy on regular review of the different information security policies(Mean=3.4, coefficient of variation =33.94 and Std deviation=1.154) and Policy on response of Information Systems security events(Mean=3.4, coefficient of variation =34.32 and Std deviation=1.167).

Policies on Bring Your Own Device to be used at the Institution as far as Institutional data security is concerned was in line with the recommendation made by Stagliano et al. (2013) that Security policy is a crucial factor in BYOD environment because employees' activities on their personal devices may affect the overall organization's performance For example, without proper security protection, employees' personal devices could introduce viruses and malware to the organization's resources as these devices are connected and By enacting BYOD policy, organizations should be able to control resources that can be accessed by employees and set priority of information to be delivered to employees . So if these Institutional employees do not comply with Policies on Bring Your Own Device to be used at the Institution, then it could be a threat to Institutional data security.

Data destruction policies for the Institutional data materials that contain sensitive information was also in line with National Information Security Policy (2014) which requires All organizations using portable and removable media must adopt formal procedures to prevent the unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities

IV. CONCLUSION

The study discovered that the following Policy were not partly implemented ; Policy on Bring Your Own Device to be used at the Institution as far as Institutional data security is concerned which is not in line with the recommendation made by Stagliano et al. (2013) that Security policy is a crucial factor in BYOD environment because employees' activities on their personal devices may affect the overall organization's performance For example, without proper security protection, employees' personal devices could introduce viruses and malware to the organization's resources as these devices are connected and By enacting BYOD Policy, organizations should be able to control resources that can be accessed by employees and set priority of information to be delivered to employees . So if these Institutional employees do not comply with Policies on Bring Your Own Device to be used at the Institution, then it could be a threat to Institutional data security.

Data destruction Policy for the Institutional data materials that contain sensitive information was also partly implemented which must be in line with National Information Security Policy (2014) which requires All organizations using portable and removable media must adopt formal procedures to prevent the unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities. The study recommends that institutions should constantly revise ICT policies in accordance with technological changes for example Policy use of mobile devices, cyber security, use of social media among others.

V. ACKNOWLEGEMENT S

This work could not have been possible without the financial assistance and moral support given by the Staff development scheme of Kampala International University more especially, the Chairman Board of Trustees Mr. Hassan Basajjabalaba The Doctoral committee members who inspired for continuous encouragement of this work despite the odds, and above all read through the work paragraph by paragraph and directing till the end. You are real mentors. Finally the authors would like to thank the Universities for giving me permission to collect data from the staff members and Private University management for allowing me use the University as my Unit of analysis. The authors also wish to thank all respondents who gave of their time to participate in our survey are also appreciated.

REFERENCES

1. *Bogere Ayub,Faruque A. Haolader,Mohammad Mahbubur Rahman(2013) The Influence of ICT Security to Academic Environment at Universities, Case Study Uganda : international Journal of Innovative Research in Science, Engineering and Technology Vol 2. ISSN: 2319-8753*
2. *Bristol University (2014) Information Security Policy*
3. *George Washington University (2014) Information Security Policy University*
4. *Gillham, B. (2000). Developing a questionnaire. The pros and Cons of Questionaires New York:*
5. *Loch, K.D., Carr, H.H., and Warkentin, M.E. 1992. "Threats to Information Systems: Today's Reality, Yesterday's Understanding," MIS Quarterly (16:2), pp. 173-186.*
6. *National ICT Policy for Uganda, 2012*
7. *National Information Security Policy (2014) NITA-Uganda*
8. *National Information Security Strategy (2011) Ministry of Information and Communications Technology, Uganda*
9. *Ndejje IT Services (NIS) Laboratory Security Policy (2008)*
10. *Nita U 2010, ICT Policies, Strategies And Initiatives Put In Place In Uganda*
11. *Stagliano, T., DiPoalo, A., and Coonnelly, P. 2013. "The Consumerization of Information Technology," Graduate Annual (1:1), p 10.*
12. *Uganda Internet Governance Forum (2012) https://www.intgovforum.org/cms/2012/Regional-%20National%20IGF/upload/2012%20National%20%20IGF%20report-1%20copy.pdf*
13. *Thomas r. Peltier, 2005, s e c u r i t y m a n a g e m e n t p r a c t i c e s. Retrieved from http://infosectoday.com/articles/peltier_awareness.pdf on 31st august 2016*
14. *Stagliano, T., DiPoalo, A., and Coonnelly, P. 2013. "The Consumerization of Information Technology," Graduate Annual (1:1), p 10.*