Analysing Information Systems Security In Higher Learning Institutions Of Uganda

Mugyenyi Raymond

Abstract: Information communication technology has increased globalisation in higher learning institution all over the world. This has been achieved through introduction of systems that ease operations related to information handling in the institutions. The paper assessed and analysed the information systems security performance status in higher learning institutions of Uganda. The existing policies that govern the information security have also been analysed together with the current status of information systems security in Uganda. Citations related management of information systems, security and policies have been identified and analysed. A proposed model illustrating the effective management of information in higher learning institutions have been developed. Relevant recommendations and conclusions have also been developed.

Key words: Information systems Security, Information Security Policy, Higher Learning Institutions

INTRODUCTION

With today's increased Globalisation inspired by rapid growth of Information Communication Technologies (ICTs), most of higher learning institutions in developed countries have managed to ease their day to day operations of handling students and staff related information while ensuring higher standard levels of security with their systems. The globalisation rate is still in its lower levels in Higher Learning Institutions of developing countries and/or even not yet at all in under developed countries. These countries lag behind in handling information security for institutional staffs and students due to low level of information technology being supported by limited finances and technical know-how. Many countries in the world still are without sufficient regulation and/or enforcement to protect user's data and privacy (Johnson etal. 2014). The purpose of this paper is to assess and analyse the information systems security performance status as well as providing recommendations for improvement of education service delivery in higher learning institutions in developing countries with major emphasis on Uganda. Uganda one of developing countries in Africa, has invested some efforts in trying to catch up the technology as Information communication Technology (ICT) is applied in almost all of its higher learning institutions to provide good security for their information against being mishandled. The estimated rate at which ICTs are being used in Uganda is at 50% increase every year (UCC, 2012). Unpleasant side of it, is that the standard at which ICT is being utilized to ensure information security is still inefficient which has played a big role in contributing towards further mishandling of data and information by both authorised and non-authorised users for their own interests.

- *Mugyenyi Raymond is currently pursuing Doctorate of Information Systems at Atlantic International University, Honolulu, USA, Tel: 256772619809 Email: rayzafrika@gmail.com*

As the number of IT increases in sophistication and complexity, the number of threats and vulnerabilities that related to the Information Systems Security (ISS) also rises up challenging the organizations in securing their business information (Karyda et al. cited by Adel Ismail AlAlawi etal, 2016). Given the widespread adoption of computer technology for business operations, the problem of information protection has become more urgent than ever (Bogere Ayub et al, 2013). It is on this basis that most of higher learning institutions most especially in developing countries suffer problems of cyber threats related to information hacking which contribute to their down fall and dissatisfaction of their clients. Universities face a variety of cyber security threats and a growing challenge from advanced, persistent and targeted threats that reflect the sector's important contribution to innovation and economic development (Universities UK, 2013).The primary risk from the different types of cyber threat to university institutions, that prevent them from going about their work are; theft of information or damage to networks, loss of access to essential data or data become corrupted as well as information being stolen, without the owner's knowledge (Universities UK, 2013).

HIGHER LEARNING INSTITUTIONS IN UGANDA

Higher learning institutions are institutions both private and public that train/teach students after high school and award them with certificates, diplomas, degrees, masters and PHD on course completion. Higher learning institutions include but not limited to Universities, colleges, and training institutes, among others. In a very simplistic view, higher learning education refers to those aspects of education that are provided in post-secondary institutions despite the lack of agreement on the curriculum to be followed (Michael Kariwo etal, 2014) Higher education is generally seen as a major (potential) catalyst towards sustainable development, in particular through its traditional missions of education, research and public service (Barth, M., G. Michelsen, cited by Waas Tom, 2012). As illustrated below;

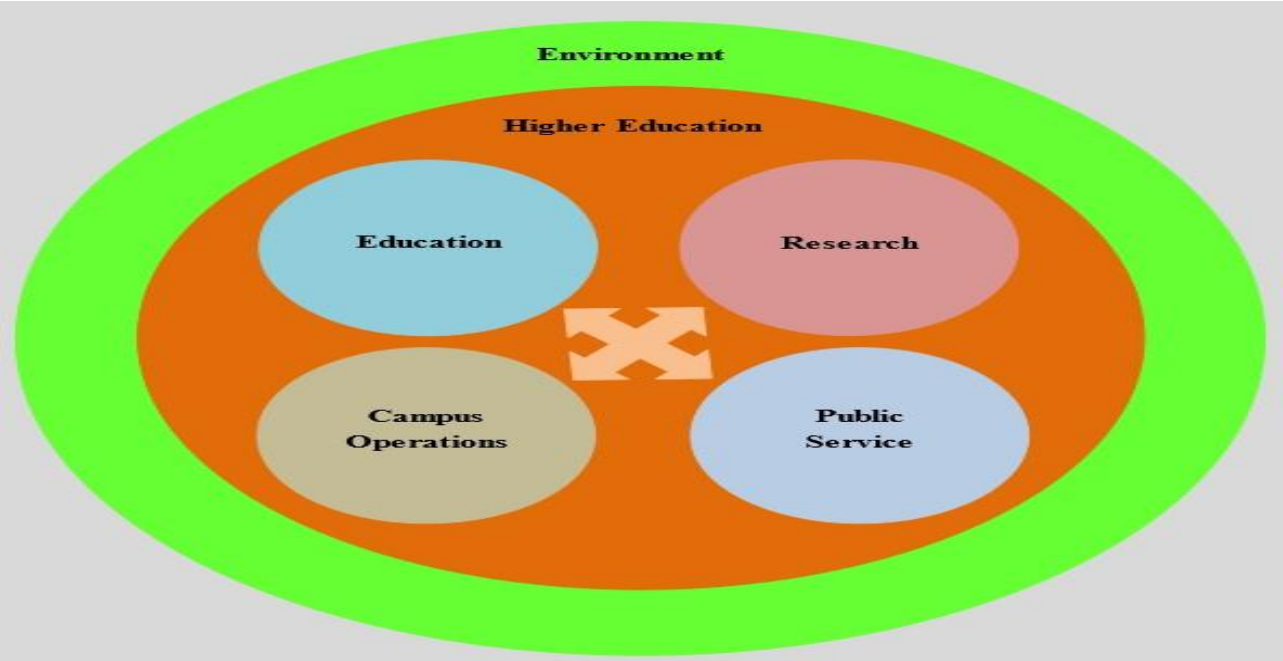

Figure 1: *High learning education as catalyst towards sustainable development source: Waas Tom, 2012*

Higher education represents a critical factor in innovation and human capital development and plays a central role in the success and sustainability of the knowledge economy (Dill and Van Vught, cited by Karine et al, 2012). They are not just tertiary schools, but they are the platforms of redistributing the traditional power and creating a new order and rank system of a society, at the same time creating and disseminating global knowledge, developmental insights and activities into societies by literally moving brains in and out of the country (Seppo Hölttä, et al 2015). An Economist Intelligence Unit report produced for the British Council January 2015 also emphasized that access to information is now freely available online; with smart phones, tablets and an array of digital tools at their fingertips, the habits and expectations of students have changed. These contributions have benefited not only students, but they have played a big role to improve on economic and sustainable development in developing countries. Higher learning institutions in Uganda are characterized by huge number of operations that are handled concurrently which puts most of their information at a risk of being lost or mishandled. The rate of students' enrolments in these institutions is also increasing rapidly, and it is on this ground that the management and utilization of information is still a big challenge. For a higher education institution where a large amount of student information is hosted student administrative systems, learning management systems and platforms any information leakage or loss would have large impacts (Cheung S.K.S, 2014). Most of the higher institutions are still lacking standard information management systems to handle their information due to limitations related to high costs, skills and corruption involved. However more efforts are needed to ensure adoption and implementation of good quality security systems to manage their information. Governments need to steer their higher education institutions toward a more balanced higher education system and these institutions should be able to respond to the national and global needs for internationalization, knowledge society and innovation capacity (Seppo Hölttä et al 2015).

INFORMATION SECURITY POLICY

Information security works under the principles of confidentiality, integrity and availability. Effectiveness in security policy performance is very crucial and it should serve for the benefits of the organisations and the government as well. Therefore Public research institutes should adopt or implement policies, regulations, processes, organizational structures, services and technology, guided by their Information Security Governance structure (Albuquerque Junior & Santos, 2014) Cheung S.K.S, 2014 explained the above three principles of information security as follows;

- Confidentiality is the ability to protect information from unauthorized accesses. For example, the use of another person's account and password to access an online banking system, which he or she does not possess the necessary access rights.
- Integrity is the ability to protect information from undetected modification or deletion. For example, in an e-mail communication, some information in the e-mail message is intercepted, modified or omitted during the message sending process.
- Availability is the ability to protect information from attacks denying or inconveniencing authorized accesses.

The framework for National Information Security involves five important levels of which the more relevant ones to the higher learning institutions are security governance and information security that en sure sufficient information handling most especially to multipurpose organizations. For the best performance of information security policy, persistent analysis of relevant policies is vital to identify most relevant information and critically handle it so as to

serve its purpose without disruption. An example of information policy analysis is illustrated in the figure below;

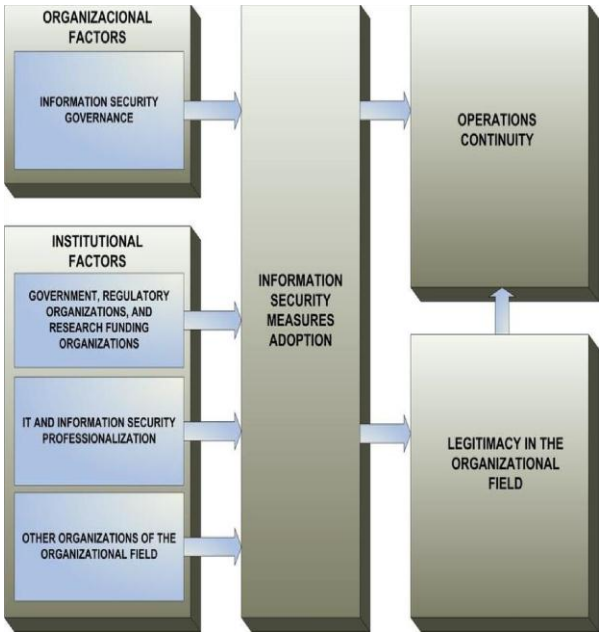

Figure 2: *Analysis model.* ***Source****; Albuquerque Junior & Santos, 2014.*

Uganda has developed a number of policies to govern the management of information in higher learning institutions of which some are already implemented and put to use, and others have not yet been implemented. According to Bogere Ayub, on cyber security management, Uganda has operationalized cyber laws, including the Computer Misuse Act (2010), Electronic transactions Act (2011) and the Electronic Signatures Act, 2011, Attendant draft regulations for the Electronic Transactions Act and the Electronic Signatures Act have been developed. Bogere further noted that the ICT ministry together with NITA-U is developing an awareness strategy to the public. National Information Technology Authority-Uganda, 2014 highlighted the guiding principles that influence actions and decisions within the information security policy as explained below;

Top Leadership Accountability: The first principle is that the most senior person in the organisation must assume ultimate accountability for information security. Cabinet Ministers should ensure that ministries, departments, authorities, and local governments (MDALs) report on their information risk position at least annually.
Collective Responsibility: The principle requires all individuals to accept a collective duty to contribute to efforts to ensure that critical infrastructure assets and services obtain protection commensurate with their value, sensitive and criticality to their organizations.
Personal Accountability: Individuals must understand and accept personal accountability for safeguarding the assets entrusted to them and expect to answer for and/or face sanctions for breaching security rules
Risk Management/Proportionality: Organizations must adapt security controls to their circumstances in particular their business needs, risk appetite, value and sensitivity of their information.
Secure/Assured Sharing: This principle requires organizations to apply suitable security controls to enable the secure sharing of information regardless of its form and method of transfer.
Suitable, Trustworthy and Reliable Staff: Organizations must only hire staff after verifying that their character and personal circumstances are such that they can be trusted with access to vital IT assets
Resilience: This principle requires organizations to build capacity to withstand and recover from cyber-attacks and disruptions in a timely manner with minimal damage

INFORMATION SYSTEMS SECURITY

Information is an asset that like other important business assets, essential to an organization's business and consequently needs to be suitably protected. This is especially important in the increasingly interconnected business environment. As a result of this increasing interconnectivity, organisations' information gets exposed to a growing number and a wider variety of threats and vulnerabilities. Information systems are interrelated components working together to collect, process, store, and disseminate information to support decision making, coordination, control, analysis, and visualization in an organization (Prentice-Hall, 2012). (David T. Bourgeois, 2014) explained the five different components of information systems as below;

- **Hardware.** The part of information system one can touch, for example Computers, keyboards, disk drives, iPads, and flash drives.
- **Software.** Is a set of instructions that tells the hardware what to do. Software is not tangible. When programmers create software programs, what they are really doing is simply typing out lists of instructions that tell the hardware what to do.
- **Data.** Data is a collection of facts and like software, data is also intangible. By themselves, pieces of data are not really very useful, but aggregated, indexed, and organized together into a database, data can become a powerful tool for businesses.
  Organizations collect all kinds of data and use it to make decisions.
- **People.** From the front-line help-desk workers, to systems analysts, to programmers, all the way up to the chief information officer (CIO), the people involved with information systems are an essential element that must not be overlooked.
- **Process.** A process is a series of steps undertaken to achieve a desired outcome or goal. Information systems are becoming more and more integrated with organizational processes, bringing more productivity and better control to those processes.

One of the roles of information systems is to take data and turn it into information, and then transform it into organizational knowledge (David T. Bourgeois, 2014). When dealing with Information Systems (IS) for the different institutions, maintaining Information Systems Security (ISS) among the employees, in the form of Information Systems Security Awareness (ISSA), is extremely important to protect the institutions' IS (Adel Ismail Al-Alawi etal, 2016). Concerning the universities, protecting personal information

for students and employees is crucial in applications regarding student information system, employee information system and other applications such as financial applications (Drevin et al, cited by Adel Ismail Al-Alawi etal, 2016) Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities. (Farah etal, 2016,) defined Information Security as the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption. Information security is also defined as a set of strategies for managing the processes, tools and policies necessary to prevent, detect, document and counter threats to digital and non-digital information (Margaret Rouse, 2016). Improved techniques for advanced and faster handling of data and information systems security management can play a great role towards efficiency and effectiveness of service delivery in the performance education sector while fostering equitable access to modern communications technologies. Information security aims at protecting the information assets of an organization from any unauthorized access, disclosure and destruction (Cheung S.K.S, 2014). Information security can best be achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures such as software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. Information security responsibilities include establishing a set of business processes that will protect information assets regardless of how the information is formatted or whether it is in transit, is being processed or is at rest in storage (Margaret Rouse, 2016)

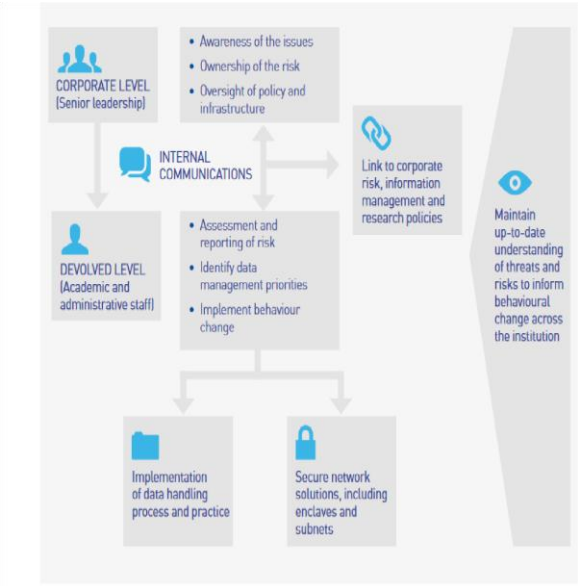

Figure 3: *Process model for managing cyber security threats in higher education institutions (University UK, 2013)*

STATUS OF INFORMATION SYSTEMS SECURITY IN UGANDA

With the increase in internet by the end of 2011, many teachers in universities of Uganda increased the utilization of internet which now calls for security concerns to maintain the technology introduced (Bogere Ayub et al, 2013). This has encouraged the rise of activities related to evaluation, assessment and analysis of information systems security usage and corresponding performance outcomes in higher learning institutions to ensure quality sustainability of their performance. The government of Uganda has tried its best to introduce a number of ICT institutional reforms to stabilize and rehabilitate the information cyber security in many sensitive departments of higher learning institutions so as to curb the recurring issues of information mismanagement. The Uganda Internet Governance Forum report (2012), also confirmed it that Uganda made some progress in implementing some key Internet Governance issues related to affordability and access to cyber security management and critical Internet resources. In addition, Uganda has developed and implemented a number of laws governing information security which include but not limited to; the Computer Misuse Act 2010, Electronic transactions Act 2011, the Electronic Signatures Act, 2011, among others. It is however unfortunate that these laws have not succeeded in ensuring the quality service delivery related to effective information management. The failure has been supported by a number of issues like limited knowledge and skills, greedy for money/ corruption, high costs involved in installing the cyber security systems, etc. The country also developed Security governance policy that focuses on all the activities required to manage information, personnel and physical security using Plan-Do-Check-Act (PDCA). (NITA-U, 2014) This has to some extent ensured better handling the information of the universities' clients and in a faster manner. The model structure of the security governance processes is illustrated below;

Figure 4: *model structure of the security governance processes* ***Source:*** *NITA-U, 2014;*

However, Information management is still a big challenge to the higher learning institutions of the country because Uganda has not yet developed Information Systems Security policies and strategies to guide its Information Technology and data management operations including standardization of work processes, infrastructure and facilities (hardware, software and system maintenance), provision of access to shared facilities e.g. administrative tools and connectivity. Uganda remains acutely short of policies and initiatives aimed at enabling mass ownership of connected devices, and there is also a shortage of coordinated efforts to exploit ICT sector opportunities (Ali Ndiwalana and F.F. Tusubira, 2012). This has not enabled the education sectors in the country to maximize benefits from application of ICT and enjoy the accompanied cost effectiveness. Most of Higher learning institutions in Uganda, are still threatened with suspicion and cyber-attack to their information systems while handling data management and information sharing. many incidences of information attack related to misusing and hacking into systems still exist in these institutions aiming at altering student marks, fees defaulters sneaking on graduation lists, poor management of students' payments details among others, are being done by both authorised and unauthorised users depending on their interests. Higher learning institutions in Uganda most especially Universities, have managed to develop some guiding policies in providing good security of their information in such a way that the information is handled by right people and utilized effectively. The institutions are have adopted to Encryption System, to protect institutions with physical security measures, digital rights management systems which prevent unauthorized use and Access Control Systems to control access to information and computer systems (Bogere Ayub et al, 2013). Ali Ndiwalana and F.F. Tusubira, 2012) identified the guiding principles for the national ICT policy In Uganda as below:

- Enhancing private public partnership in delivery of ICT infrastructure and services
- Ensuring universal access to basic ICT infrastructure
- Technology neutrality of ICT services
- Integrated ICT facilities and services consistent with technological convergence
- Globalization: The policy implementation shall take into consideration developments at the global level so as to capitalize on latest trends in ICT
- Addressing cross cutting issues in ICT such as sustainability, gender, youth and people with disabilities;
- Promoting cultural diversity and identity, linguistic diversity and local content;
- Providing enterprise oriented and consumer-centric services

NITA-U, 2014 also advised on minimum requirements for securing Information Sharing within organizations as given below; (a) Identify and record risks involving external parties; (b) create information exchange policies and procedures; (c) use formal exchange agreements such as codes of connection and memoranda of understanding; (d) assess compliance of exchange partners at least annually or when required; and, (e) disconnect/end sharing with non-compliant entities Last year, Uganda realized many incidences of ICT security threats at one of the leading and the oldest universities (Makerere University) where a good number of Ghost students appeared on the graduation lists and leaving out the genuine students who had successfully completed and fulfilled the minimum requirements for graduation. This was as a result of loopholes in the systems that enabled lecturers to alter the student marks to accomplish their personal interests e.g. sex, money among others. University Students on the other hand, are reproducing/ duplicating universities' academic documents and present them to get employment as well as using them for admission for upgrading in different institutions. Another incidence happened to parliament where many members of parliament aspirants used forged documents to be voted and even happened to succeed in winning the races and even sworn in but were later thrown out of parliament by courts of law.

PROPOSED INFORMATION SYSTEM SECURITY FOR HIGH LEARNING INSTITUTIONS IN UGANDA

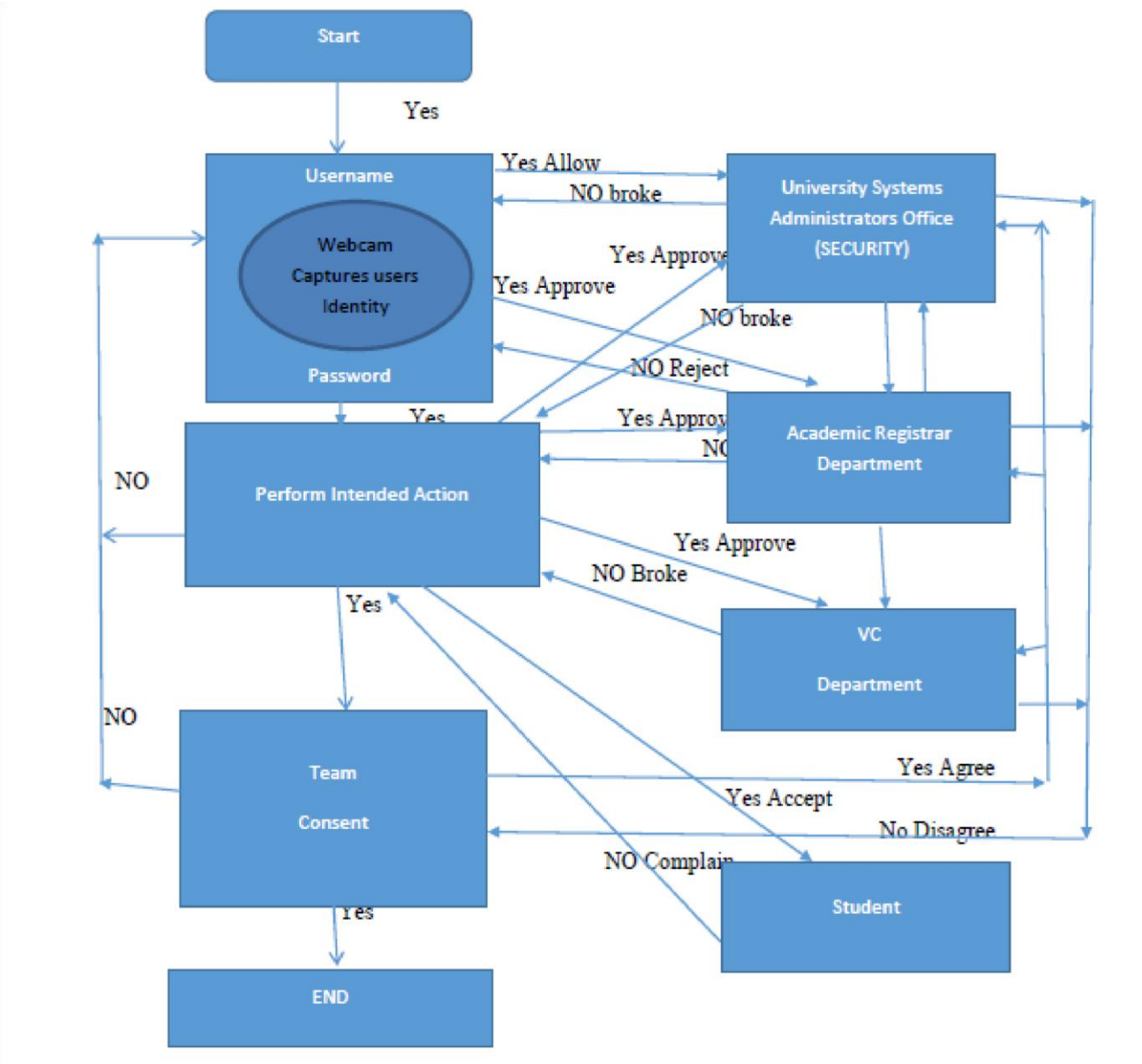

Figure 5: *A proposed model,* ***Source;*** *Mugyenyi Raymond*

RECOMMENDATIONS

Higher investments in information systems security is highly recommended in learning institutions especially in developing countries to improve on the quality of their education. Much emphasis should be put in developing suitable cyber security models that aim at ensuring effective information security controls at in all relevant areas of the institutions for quality assurance. The developed models should designed in such a way that they are able to work hand in hand with the implemented policies of the institutions to achieve the institutions' goals in a cost effective manner. The government should ensure implementation of strict laws and policies to protect all information for the institutions from being mishandled by either authorised or unauthorised users so as not to be replicated, stolen, or other different practices that are not good to the information. The laws and policies should be monitored periodically using risk assessments guidelines and regulated depending on demanding conditions. Information security measures such as mantraps, encryption key management, network intrusion detection systems, password policies and regulatory compliance (Bogere Ayub et al, 2013) among others should be developed and implemented to increase the security performance of information systems for higher learning institutions. The information systems security must contain the highest performing capacities to detect any changes that occur to the information and effectively handle any negative effects occurring to the information. The universities in Uganda should consider producing documents that will have a certifying link on their websites where organizations, company's universities among others will keep verifying the originality of the documents presented to them. Capacity building among students, teaching and nonteaching staff should be encouraged to equip them with relevant skills to handle the systems and ensuring effective information sharing and management

CONCLUSIONS

Information is the vital asset that cross cuts in almost all organisations, which requires critical attention in its management i.e. capturing, storing, retrieval, utilisation and sharing. It is however important to note that information management has continuously become a challenge to many organisations most especially those that handle multitask operations like higher learning institutions that deal with large number of students and staff members. Information communication technology (ICT) have been identified as the best tool that can handle information either for large or small organisations very effectively and in a cost effective manner. ICTs are very relevant in curbing the information security threats in higher learning institutions, since they have the potential to ease the day to day operations of handling students and staff related information while ensuring higher standard levels of security with their systems. The government of Uganda appreciated the benefits of ICT services to the higher learning institutions which prompt it to adopt to deployment and application of these services it most of its organisations most especially higher learning institutions. The government has taken an extra mile to develop and implement a number of policies and strategies that govern and protect the performance of these systems in her organisations. Important to note is that an awareness strategy to the public about ICTs has been developed by ministry of ICT which is expected to bring a lot changes towards improved standard management of information. In specific higher learning institutions of Uganda like Makerere University, a number of incidences result from information mishandling due to poor information systems security, have occurs and costed both individual, organisations and the government as well. Information systems security plays a vital role of ensuring effective protection of all the information for the higher learning institutions to avoid the negative implications related to information mishandling like duplication, and disappearance. It is therefore equally important to employ multiple security controls and policies to completely get lid of security threats that lead to information distortions. A proposed model for information System Security for High Learning Institutions in Uganda has therefore been developed to ensure effectiveness in information management.

REFERENCES

[1] Adel Ismail Al-Alawi, Sulaiman M.H. Al-Kandari and Refaat Hassan Abdel-Razek ,2016;

[2] Albuquerque Junior & Santos, 2014; Adoption of information security measures in public research institutes.

[3] Ali Ndiwalana and F.F. Tusubira, 2012; what is happening in ICT in Uganda; A supply- and demand- side analysis of the ICT sector; Evidence for ICT Policy Action.

[4] An Economist Intelligence Unit report produced for the British Council, 2015; connecting universities: Future models of higher. Education; analyzing innovative models for Afghanistan, Bangladesh, India, Nepal, Pakistan and Sri Lanka.

[5] 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.

[6] Cheung S.K.S. (2014) Information Security Management for Higher Education Institutions. In: Pan JS., Snasel V., Corchado E., Abraham A., Wang SL. (eds) Intelligent Data analysis and its Applications, Volume I. Advances in Intelligent Systems and Computing, vol 297. Springer, Cham

[7] David T. Bourgeois, 2014; Information Systems for Business and Beyond; https://bus206.pressbooks.com/chapter/chapter-1/. Evaluation of Information Systems Security Awareness in Higher Education: An Empirical Study of Kuwait University

[8] Farah Nurafiqah Hanis binti Abd Hadi, Akram M. Zeki, 2016; ICT Readiness and Information Security Policies in OIC Countries

http://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2013/cybersecurity-and-universities.pdf
https://www.researchgate.net/publication/261063232_Information_Security_Policy_Compliance_in_Higher_Education_A_Neo-Institutional_Perspective

[9] Johnson, J., Lincke, S. J., Imhof, R., & Lim, C. (2014). A comparison of international information security regulations

[10] Karine, Tremblay, Diane, Lalancette, Deborah and Roseveare, 2012; Assessment of Higher Education Learning Outcomes; Feasibility Study Report Volume 1. Design and Implementation

[11] Mahfizah Mazlan, Nurul Aqilah Mohd Zarani, Jamaludin Ibrahim, 2016; A Cyber Security Assessment of Muslim Countries

[12] Margaret Rouse, 2016; Managing information security amid new threats: A guide for CIOs; http://searchsecurity.techtarget.com/definition/information-security-infosec.

[13] Michael Kariwo, Tatiana Gounko and Musembi Nungu (Eds.), 2014; A Comparative Analysis of Higher Education Systems

[14] National Information Technology Authority (NITA) Uganda, 2014; National Information Security Framework (NISF) Publication National Information Security Policy.

[15] Prentice-Hall, 2012; Excerpted from Management Information Systems, twelfth edition. 16. Seppo Hölttä, Annica Moore, Elias Pekkola, 2015; Higher Education Institutions. Partnering for Development and Change. Reflections of the First Round of the Finnish HEI ICI Programme. Centre for International Mobility CIMO & University of Tampere.

[16] R., Wright, T. (2012) Sustainable Higher Education –Understanding and Moving Forward. Flemish Government –Environment, Nature and Energy Department, Brussels.

[17] Universities UK, 2013; Cyber security and universities: managing the risk.

[18] Waas, T., Hugé, J., Ceulemans, K., Lambrechts, W., Vandenabeele, J., Lozano,