An Analysis of Information System Security of a Ghanaian University

Ephrem Kwaku Kwaa-Aidoo*, Mathias Agbeko**

*Department of ICT Education, Faculty of Science Education, P. O. Box 25, Winneba-Ghana

**Department of ICT Education, Faculty of Science Education, P. O. Box 25, Winneba-Ghana

‡ Ephrem Kwaku Kwaa-Aidoo; Department of ICT Education, Faculty of Science Education, P. O. Box 25, Winneba-Ghana: Tel: +233206724609, e-mail: ekkaidoo@uew.edu.gh

Abstract - Information Systems in Universities are set up to address several requirements, ranging from openness, flexibility, scalability and performance to security and privacy as well as support the key role of teaching, learning and research. This paper analyses the information system environment of a public Ghanaian university and discusses the state of information security. It discusses the short falls, and some improvements that may assuage the identified risks. This is a descriptive research informed by a pragmatist viewpoint. The study focused on technical and non-technical staff of the university. In all, 180 respondents were stratified into technical and non-technical users. The results indicated that respondents viewed confidentiality as the most important information security objective followed by integrity and availability. The university assets that respondents viewed as most valuable were students records and research data as compared to computers and mobile devices. Respondents also indicated that they experienced malware attacks frequently with very few experiencing unauthorised change of information on systems. It is recommended that there should be regular training programs to create awareness on cyber security threats among stakeholders especially within a typical BYOD (Bring Your Own Device) environment such as a university. In addition, security policies on antiviruses should be developed, implemented and enforced to ensure protection of sensitive data.

Keywords: Information Systems, Information Security, Malware, Confidentiality, integrity

1 Introduction

Universities and other institutions of higher learning usually maintain various databases that support their operations. These include personal information of their students for managing student admission, registration, study, examination, graduation, recruitment and other student services such as accommodation and careers.

These information systems regularly come under attack because of the nature of the systems and the environment they operate in [1]. Information systems in Universities are unique as a result of the nature of their user characteristics and their usually complex information technology infrastructure and this invariably affects security management [2]. As has been argued by many, technology is impacted by users and by organizational culture [3, 4]. Though many users embrace technological innovations, some individuals mistrust technology and some have not learned to use it whilst others feel it slows them down. Irrespective of the reason, it is noteworthy that many people will try to sidestep technical controls [5] whilst others might deliberately attempt to sabotage information systems.

In this regard, to ensure that information is secured, it is important to understand the context within which the information system operates. The information security ecosystem in higher educational institutions include various resources and have generally been described at various levels. Universities manage various IT resources, these include People (IT staff, user support,

programmer analysts), Data/Information (e.g., electronic records, databases), IT Infrastructure Systems (e.g., departmental billing systems, student records), Software (e.g., "productivity" software) and Hardware (e.g., servers, desktops, laptops) [6]. This environment is however unlike what pertains in the corporate world and this is because of the nature of the environment, funding available for managing security, requirements to be met and the organizational infrastructure.

2 Objectives of the Research

The objective of this work was to obtain an understanding of information security threats and risks within a typical higher educational institution for the purposes of recommending improvements to its management. The study aimed at examining the level of security awareness within a Ghanaian public University. It also assessed the preventive measures in place. Specifically, the research work is aimed at:

1. Establishing a shared understanding of threats and risks across the institution

2. Identifying and evaluating information assets for their potential cyber security risk

3. Understanding and evaluating the different information security needs and practices of the University and users.

3 Assessing Information Security Within Organisations

Information security has been described as "*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*" [7]. The British Standards Institution in [6] argue that information security is primarily a management or business issue and not a technical problem. In other words, technology is rather the tool to be used for achieving security. This is in line with the view that security is generally a weakest link problem and humans are the weakest link [8-10]. It is generally part of a larger social system and not a self-fulfilling function of an organisation. Security must therefore be approached as a social problem because the mechanisms, architecture and even the information asset that is protected arises as an outcome of a compromise between various stakeholders.

Information Security Risk Assessment (ISRA) is used to identify and prioritize information assets. It is also used to identify and monitor the specific threats that an organization is exposed to. Normally ISRAs involve three distinct phases which are context establishment, risk identification and risk analysis [11]

Risk assessment involves two key phases and the first involves defining the scope of the risk assessment exercise, identifying information assets and determine and prioritize risks to the assets. The second phase which is risk management involve making decisions on controlling the identified risks.

The focus of this work was on the organizational context that sets university environments apart from other organisations and businesses. According to Shamala et al [10], in assessing the organizational context, most of the methodologies used for information security risk assessment involve a look at the objectives/goals of the organisation, scope and boundary of the security review, a SWOT analysis, obtaining information about critical assets and current security practices/requirement.

The general interrelations surrounding securing an information system involves an asset with an owner that faces a threat of attack from an attacker. The owner normally defines the security problem which involves what protection is required and subsequently defends the asset using some security mechanism or countermeasures against the potential attack.

Aside the owner, who in this case is the university, there are many other players who are also stakeholders. These will include senior and junior members of staff within a university environment. There is however the wider environment within which the university operates. These stakeholder might have varied agenda competing or otherwise which acts as a proxy [12]. With this they negotiate the risks, tolerance

and trade-offs which should result in a security policy aimed at defending the system. In the case of the University, the main stakeholders will be users who own, control or use the data within the university. There are however powerful external stakeholders including the National Council for Tertiary Education and other regulatory regimes like the Data Protection Act (Act 438) which impact information security policy and decisions on information security trade-offs. One of the biggest challenges lie in the characteristics and the constantly changing needs of the largest user segment who are the students themselves [2]. Stakeholder interest in organizational information security could either be a regulative expectation, normative expectation or cognitive expectation and these force organisations to comply with information security requirement.

On the opposite end of the information asset owner who aims to protect the asset is the attacker. Attackers will generally attempt to bypass a security system to get access to the asset and technology can automate, enable class attacks, extend reach and aggregate data to enable attack. A security policy is therefore meant to reflect this dynamic. It codifies and define the security system made up of the security mechanisms and counter measures considering principles including in-depth defence, compartmentalization and choke points.

The attributes that are of interest in ensuring information security compliance are Organisational Culture, Operational Process, Environment and Technology [13]. Organizational culture deals with issues including management commitment, accountability, and awareness and training whilst Operational process looks at process integration, auditing and monitoring.

4 Understanding Information Security within University Environments

Provision of internet to students is arguably the biggest issue for many institutions. Universities operate in an environment that see thousands of users arrive and leave within a short period every year. To complicate this further, students are usually technologically savvy with a varied user base with different expectations in terms of performance, availability and freedom with some of them having significant hacking skills, as well as potentially mischievous inclinations [2].

University campuses encourage easy access to information to encourage knowledge transfer. It has been argued that access to university networks and systems on campus is higher than in the corporate environment [14]. They encourage openness through the dissemination of knowledge and research findings through publications. This is however conceptually opposed to the objective of security which is about restricting access to information resources. These issues are in addition to the fact that universities use cutting edge software to support research which are not well understood and could introduce risks. This coupled with Universities character of openness makes the task of securing information assets even more difficult.

5 Information Assets of Universities and Protection

An Information Asset *has been described as "a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognizable and manageable value, risk, content and lifecycles"* [15]. It is very essential to identify the information assets of an organization. Until the information assets of an organization are identified, its location and its value known, it will be worthless spending time, money and effort on information security.

Many kinds of information reside on universities networks and systems. Some of this information is publicised and would not be harmful to the University if disclosed whereas others are very confidential and would be extremely damaging if disclosed or compromised. Most information however lies between these two extremes.

These assets include commercial or politically sensitive data, sensitive information from third parties and data generated and retained for the purpose of running the University enterprise [16].

Some of these assets including personal identifiable information are usually subjected to statutory protection like data protection laws and this makes it imperative to ensure that they are protected. Consequently, a successful attack on a University's information system may result in reputational, legal, economic and operational damage. Breach of commercially valuable information will result in financial losses.

Non-military organisations usually focus on maintaining data integrity [17] to protect operational data like students and financial records in the case of Universities, however politically sensitive information, research and proprietary information produced by Universities require confidentiality instead.

Due diligence dictates that the University treats its information assets with protection commensurate with its value and purpose and universities normally classify data to reflect the value the data is [18, 19].

6 Funding Restriction in Ghanaian Public Universities

Funding for higher education has become a major issue for both developing and developed nations across the globe and Ghanaian universities have not been an exception [20, 21]. The ability of higher educational institutions to acquire enough funding to ensure the day-to-day running of the administration, teaching and research of universities has become a major obstacle and constraint to capacity building for many countries in the world. Unlike business enterprises that have substantial resources to invest into information security, educational institutions are more constrained this notwithstanding they face some of the most demanding security challenges due to the dynamic interaction between students and their IT resources.

The Government of Ghana has placed a strong emphasis on the role of ICT in contributing to the country's economy. The government has acknowledged the role of university education and the acquisition of critical skills such as teaching, engineering, medicine, among others needed for socio-economic development. There are however, ineffective flows of income, especially from the government, in support of higher education leaving a funding gap of 60% [22]. The government has clearly indicated its inability to act as the sole financier of tertiary education due to economic constraints [23, 24]. Even though money is approved and allocated in the national budget, it sometimes becomes very difficult for the universities to receive it on time due to ineffective functioning of some of the national institutions [25].

Tertiary institutions in the country have therefore, over the years been starved of both adequate development and recurrent expenditure making it impossible for them to operate at full and efficient capacity and this affects its ability to operate secure information systems.

7 Effect of the BYOD Environment in Universities

With mobile devices increasingly embedded into all parts of society, organizations are finding that their employees increasingly want to use their own personal mobile devices to conduct work (often alongside corporate-provided devices), and many are reaching out to corporate IT to support this. While employers cannot stop the use of mobile devices for both work and personal agendas, they need to know how to control it.

Bring Your Own Device (BYOD) environments enhance productivity [26], hence ensuring a secure environment for BYOD could be a source for high competitive advantage. In the Ghanaian university environment, enabling BYOD will ensure additional IT resources which otherwise cannot be provided due to the lack of resources.

BYOD alters the traditional security model of protecting the perimeter of the IT organization. This occurs as a result of distorting the definition of the perimeter; the physical location and asset ownership. Though it might seem BYOD introduces new risks, it rather expands the current risk profile. Ernst and Young [23] identify five risks relating to BYOD security as lost and stolen devices, physical access, role of end user device ownership, always on with increased data access

and lack of awareness whilst the top four security concerns are device security, data breach security, mobile data security and mobile application security.

Many users on university campuses typically have many multiple devices. As mentioned earlier, Universities by their culture maintain open networks and open access to information and are also natural BYOD environments. This environment has however come under serious challenges. Just like other organisations they come under attacks from within and outside their organization. The challenge is protecting data on devices that the institutions do not own. Breaches however could be very costly in terms of loss of valuable information including personal data of students and staff and research in various fields ranging from pharmaceuticals to computing and patents.

This situation has prompted proposals akin to a form of multilevel security. These recommendations have revolved around the audit of all the information held on these devices, including research data and student and employee personal information; categorizing them and then deciding the level of security needed [27].

8 Potential Threats and Attacks Against Universities

Threats in universities include the usual scenarios like DOS & DDOS attacks, network intrusions, botnets, e-mail viruses and phishing scams with internal threats like student hackers and social networking ploys [2]. However, according to 2014 survey of higher educational institutions in the USA, hacking accounts for most data breaches accounting for 36%. This was followed closely by "unintended disclosure" which accounted for 30% [28]. In another study identity theft was found to be the leading reason for breaches accounting for 74% and this had increased from 49% from a year before [29]. Other studies have malicious code as the greatest problem facing higher education institutions [30]. Other notable threats include ones posed by unvented applications usually installed by IT savvy students and staff running on the network.

As mentioned earlier, it is imperative to understand the information assets considered critical by the university and which of these could be targeted by attacker. The means of having authorised and unauthorised access to this information should be known and then policies and controls introduced to manage access.

9 Research approach and methods

The study was informed by a pragmatist viewpoint which has a philosophical assumption that people interpret their worlds according to the subjective meanings they direct towards phenomena. It therefore took the form of a survey is considered an effective methodology [31] and which was best suited to such research aimed at the description of phenomena. The method adopted was to allow the generation of knowledge by describing issues and characteristics surrounding information security management in the University of Education, Winneba. The University is one of the ten (10) has a total of 30,367 members of which 1,782 are members of staff constituting 5.9%. The survey collected data on the types of devices used, the information assets considered valuable, attacks that had occurred and the protection available. Additionally, some documents were consulted to collect some statistics published by the university.

The study focused on the main stakeholders identified in the university system who were the technical and non-technical users. Hence the targeted population was stratified into the two groups. The non-technical users were randomly selected to avoid bias. This sample was diverse comprising staff and students, males and females from a variety of departments belonging to different age groups. A purposive sampling method was however used to select technical staff of the University from whom data were collected. This was because some of the staff had more relevant and adequate information about the issue than others. They were appropriately chosen per their expected knowledge of the security setup of the university.

Questionnaires were used to collect data from the respondents. Two sets of different

questionnaires were administered for the Non-Technical and technical users respectively. This was because they played different roles in securing the system. A total of 180 questionnaires were administered to the non-technical users of which 4.5% of the respondents were members of staff. A structured survey was administered to three (3) technical users and they were all received. A questionnaire was developed by the researchers and validated by peer review. Suggestions were used to improve it before a final version was administered. The questionnaires were all administered in person to improve the response rate. The data was analysed quantitatively using descriptive statistics and some inferential statistics.

10 Results and Discussions

10.1 Devices owned by Respondents

Data was collected on ownership of four computing devices and whether it was provided by the University or provided for by the respondents. As shown in Fig. 1, respondents overwhelmingly owned laptops (83.9%) closely followed by smart phones (78.3%) and these were acquired by users. From Fig. 2, a third of respondents (32.6%) had desktops provided for by the University whilst under 1% of respondents used laptops, smart phones and tablets provided by the university. This indicates a typical BYOD environment which has implications for security.

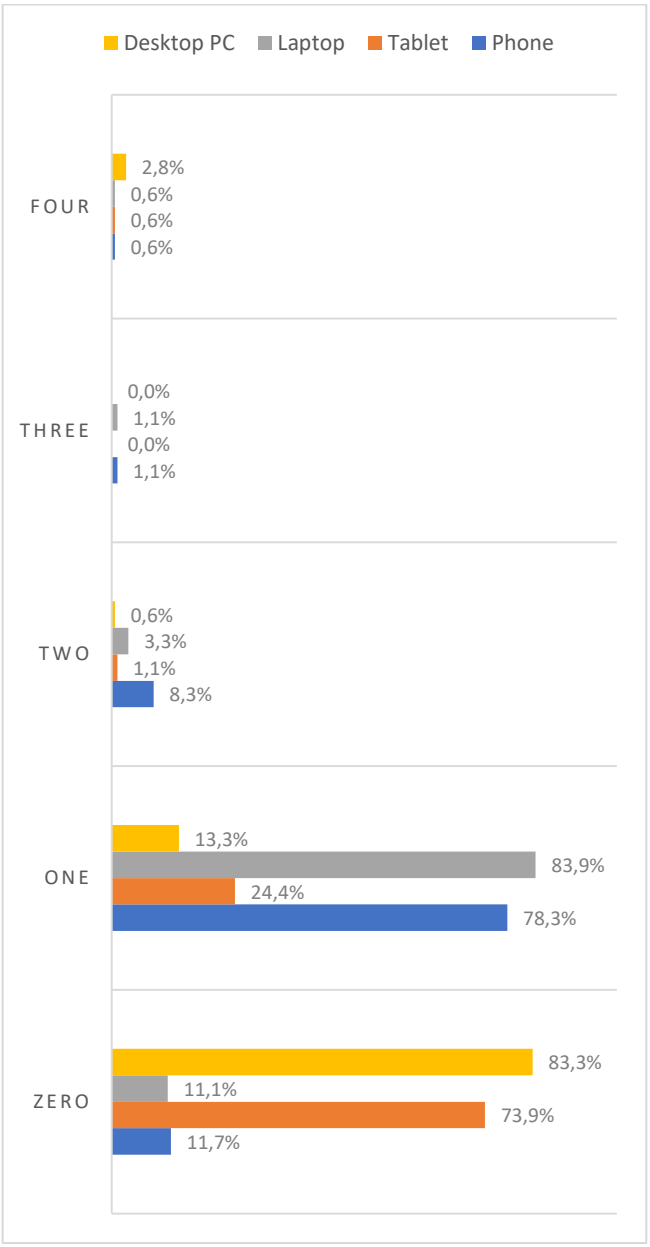

Fig. 1. Devices owned by respondents

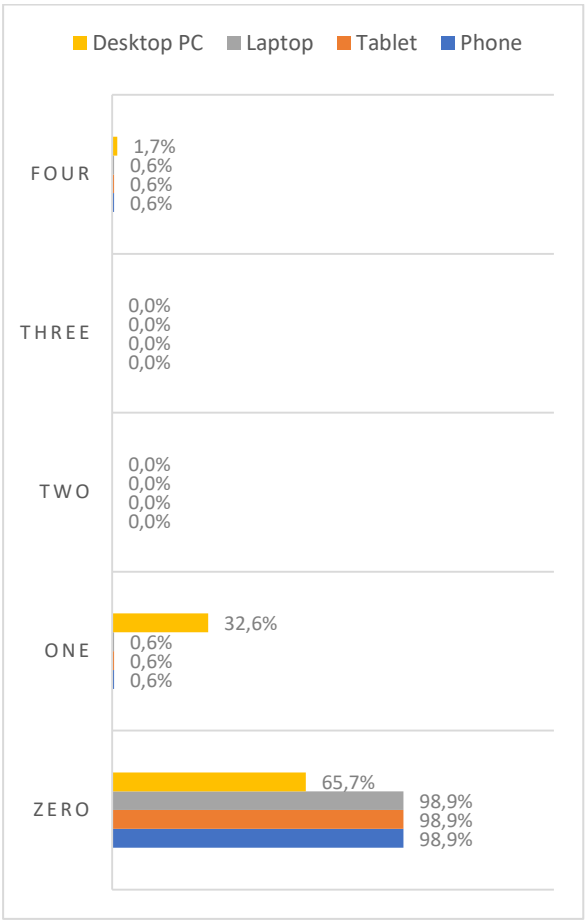

Fig. 2. Devices provided by the university

10.2 Security Objectives

Figure 3 below shows that respondents rated confidentiality at seventy one percent (71%) as the most important security objective compared to integrity which was rated at forty one percent (41%). To confirm this difference was significant a paired sample test was done with a hypothesis:

H0: There is no significant difference between integrity and confidentiality and

H1: There is a significant difference between integrity and confidentiality.

At a significance level of 0.05 the p-value was 0.003 which was outside the acceptance region hence the null hypothesis was rejected. This meant respondents valued confidentiality more than integrity. This contrasts with Clark and Wilson [17] that argues that in non-military systems, integrity is viewed as the highest priority with respondents rather viewing confidentiality as the most important information security objective. As suggested by [18, 19] some information resources require high confidentiality. However aside research finding published at conferences and in journals, the University does not produce any sensitive or proprietary knowledge and there are no registered or pending applications for intellectual property as indicated in their annual statistics hence the apparent reason for prioritising confidentiality is not existing Fig. 3 also shows that a minority of forty nine percent (49%) of respondents viewed availability as the most important security objective. Though several authors have described openness as a key characteristic of University environments the results suggest that system availability is not viewed as a primary objective.

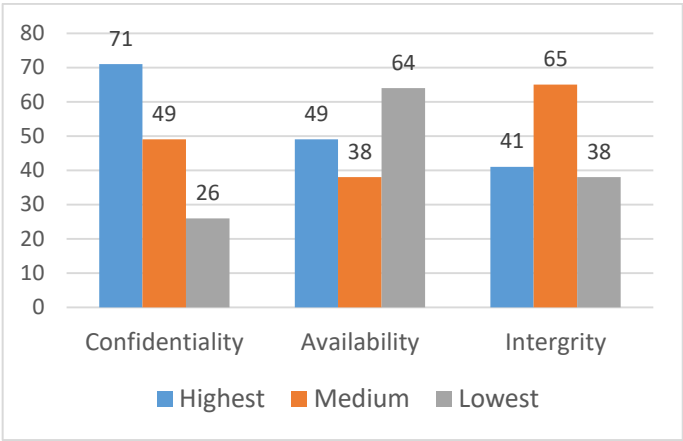

Fig. 3. Security objectives in order of importance

10.3 Experience of Cyber Attacks

The survey sought to find out the frequency of cyber-attacks experienced by users in the university. From the analysis presented in Fig. 4, an overwhelming number of respondents had not experienced cyber-attacks.

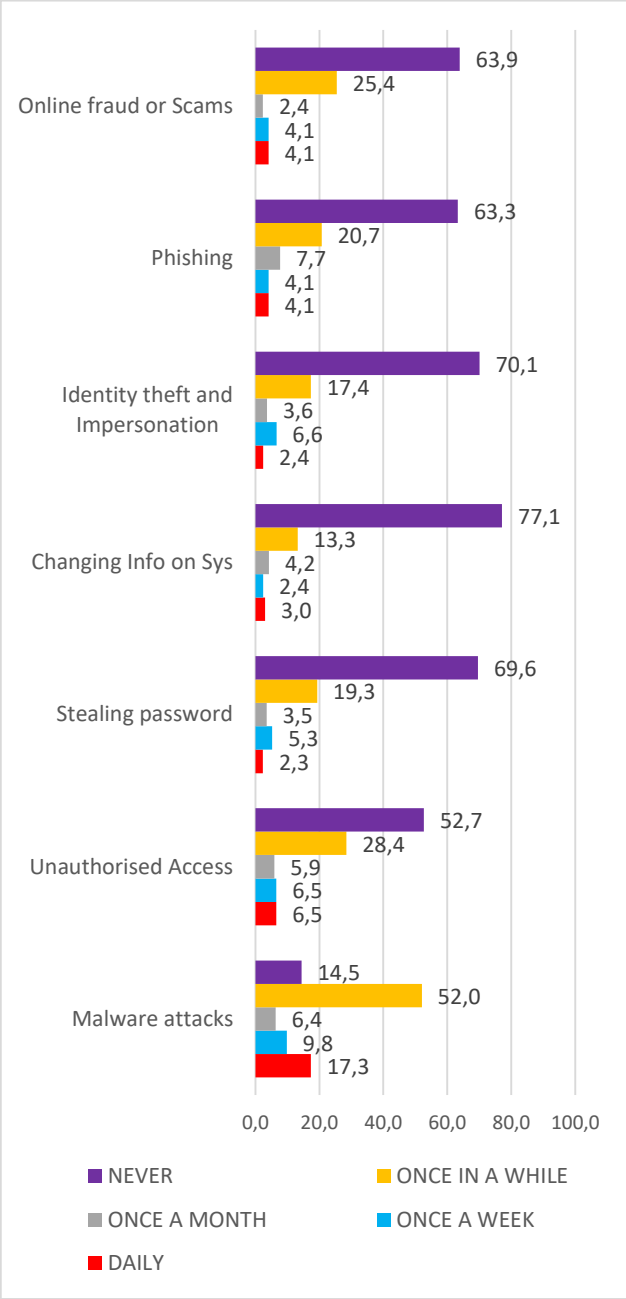

Fig. 4. Cyber/Information Security Attacks

Some had however experienced some incidents with malware being the incident that was most experienced by respondents. About 52% of the respondents experience malware attacks occasionally whilst 17.3% experience frequently.

10.4 Student Turnover

The total number of student users in the University of Education, Winneba as at 2016 was 28,585. However about 9,957, constituting 35% of users, were enrolled in 2016. This indicates that more than a third of student users leave and replaced every year. This number excludes members of staff who leave the university for various reasons and temporary staff including visiting and adjunct staff. This is a very high number having implications on user account management. This is clearly in line with observations made by AT&T [12].

10.5 Management of Security and Available Protections

Interviews with technical staff indicated that there is no high-level manager in the university with sole responsibility for managing, monitoring and or improving information security. Secondly the University had not conducted a risk assessment and technical staff did not feel there was adequate security in the University. The University only has basic security mechanisms including user account controls, firewalls, email protections and endpoint security for users.

10.6 Knowledge of Information Technology Policies

Though the technical staff indicated that there were some Information Technology policies, an overwhelming majority of respondents had little or no idea of these policies that regulate access to and use of these networks. Figure 5 below shows that 87.7% of the respondents do not know or are not sure of any policy on the access to and use of the university ICT resources. Only 15.3% of the respondents have knowledge about policy governing the use of ICT resources.

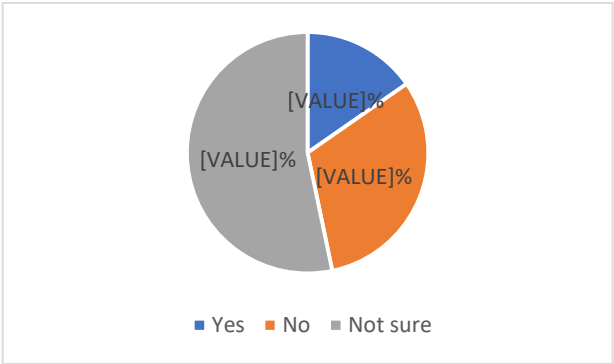

Fig. 5. Controls and Policies on Access to and Use of Networks and Data

10.7 Assets requiring protection

A breach of information asset in a university can be very costly and damaging. Due to this the

researchers sought to identify and evaluate information assets for their potential cyber security risks.

Fig. 6 shows that most respondents said that student's record is most sensitive to the university recording 71.3%. The next was internet connectivity which recorded 65.1%. Financial records, admin records and research data recorded 61.8%, 62.2% and 39.1% respectively indicating that resources that contain Personally Identifiable Information (PII) of students require more protection than staff laptops and staff mobile devices which recorded 33.3% and 24.6% respectively. This result coupled with Fig. 3 indicates that the confidentiality of personal identifiable information especially student's records appears to be of upmost concern to respondents.

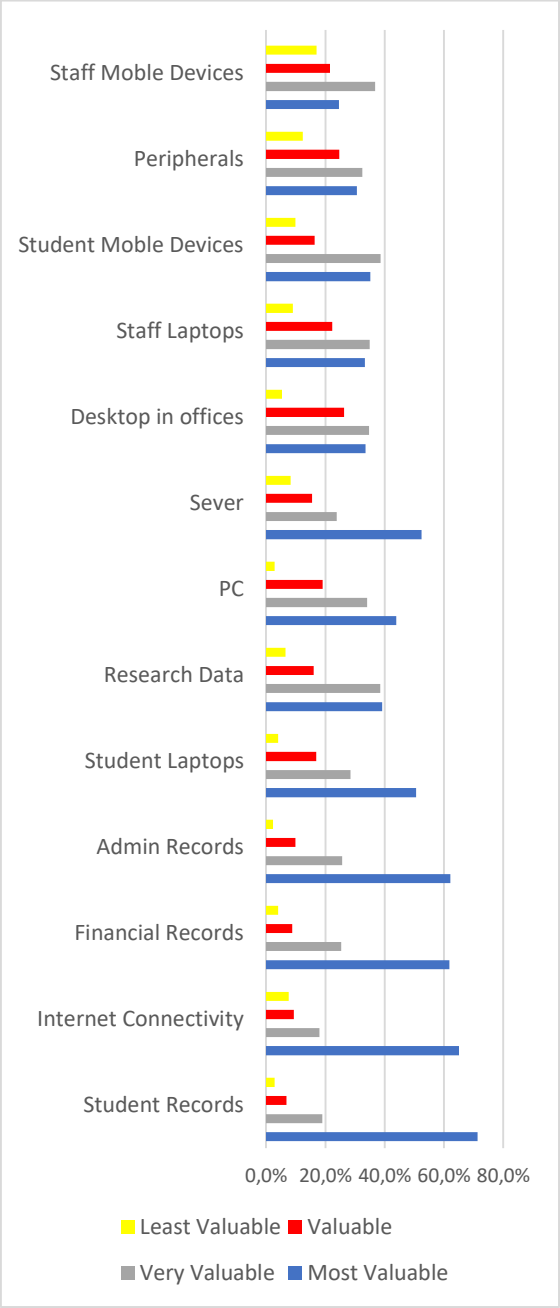

Fig. 6. IT Assets Requiring Protection

11 Conclusion

The study showed that users viewed confidentiality as the main security objective however from literature integrity would have rather been the more logical based on their choice of value of data and the types of data requiring protection. It is therefore important to educate users on the threats and how to secure them. This is more so because the survey also indicated that many respondents were not aware of security policies on information security. This requires

extensive education and implementations systems to ensure users act in ways that support the security objectives of the University. It is also very important to appoint a high-level information security officer to ensure the coordination and oversight of information security operations.

References

[1] C. E. Harris and L. R. Hammargren, "Establishing a Written Information Security Program to address exposure," Professional Media Group, Trumbull, 2016.

[2] AT&T, "Security for Higher Education," AT&T, Dallas TX, 2009.

[3] C. Holman, D. N. Harrison, and A. Swann, *Creating a Culture of Security*: The Coca Cola Company, 2011.

[4] T. Kayworth and D. Whitten, "Effective Information Security Requires a Balance of Social and Technology Factors," *MIS Quarterly Executive*, vol. 9, pp. 165-175, September 2010.

[5] ISACA, "An Introduction to the Business Model for information Security," ISACA, Rolling Meadows, USA, 2009.

[6] S. D. Franklin, "Information Technology Managing Information Assets " University of California, California, 2011.

[7] British Standards Institution, "Information Technology-Security Techniques-Code of Practice for Information Security Management " vol. BS/IEC 17799, ed: British Standards Institution, 2005.

[8] G. L. Orgill, G. W. Romney, M. G. Bailey, and P. M. Orgill, "The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems " presented at the 5th conference on Information technology education Salt Lake City, UT, USA, pp. 177-181, 28-30 October 2004.

[9] M. E. Whitman and H. J. Mattord, *Principles of Information Security*, Fourth Edition ed.: Course Technology, 2012.

[10] C. W. Flink, "Weakest Link in Information System Security," presented at the Workshop for Application of Engineering Principles to System Security Design, Boston, Massachusetts, pp. 61-68, 6-8 November 2002.

[11] P. Shamala, R. Ahmada, and M. Yusoff, "A conceptual framework of info structure for information security risk assessment (ISRA)," Journal of Information Security and Applications, vol. 18, pp. 45-52, September 2013.

[12] B. Schneier, *Beyond Fear*. USA: Copernicum Books, 2006.

[13] A. Alkalbani, H. Deng, and B. Kam, "A Conceptual Framework for Information Security in Public Organizations for E-Government Development," presented at the Australasian Conference on Information Systems, Auckland, pp. 1-11, 8-10 December 2014.

[14] J. Wolff, "Can Campus Networks Ever Be Secure?," The Atlantic Monthly Group, 2015.

[15] The National Archives, "Identifying Information Assets and Business Requirements," Open Government Licence, London, 2017.

[16] Universities UK, "Cyber security and universities: managing the risk," Universities UK2013.

[17] D. D. Clark and D. R. Wilson, "A Comparison of Military and Commercial Computer Security Policies," in *IEEE Symposium on Computer Security and Privacy*, Oakland California, pp.184-194, 27-29 April 1987.

[18] University of Wisconsin, "Information Asset Classification," University of Wisconsin, Whitewater, 2017.

[19] University of Southern Queensland, "Information Asset and Security Classification Procedure," University of Southern Queensland, Toowoomba, 2014.

[20] A. Ibrahim, "Lack of funding, a threat to quality tertiary education - Outgoing KNUST Vice-Chancellor," in *myjoyonline.com*, ed. Accra: Multimedia group, 2016.

[21] R. C. Abaidoo, "The Future of Postgraduate Education and Training in Ghana " presented at the National Summit on Tertiary Education In Ghana, Accra, pp. 2-4 November 2016.

[22] K. Adu, "Funding of Tertiary Institutions in the Era of Global Economic Challenges," presented at the KNUST Summer School, Kumasi, 2015.

[23] D. Debrah, "Financing Higher Education: Challenges for Students at the University of Ghana," Master of Philosophy, Institute for Educational Research, Faculty of Education, University of Oslo, Oslo, 2008.

[24] S. Isahaku, "An Analysis of Dominant and Alternative Approaches to Education Reform in Sub-Saharan Africa: the case of Ghana," Doctor of Philosophy, Department of Education, Faculty of Social Sciences and Technology Management, Norwegian University of Science and Technology, Trondheim, 2009.

[25] Ghana News Agency, "Teachers Criticise Government For Delayed Subventions," Peace fm, Accra, 2013.

[26] Ernst and Young, "Bring your own device: Security and risk considerations for your mobile device program," Ernst and Young, 2013.

[27] A. Gonsalves, "With universities under attack, security experts talk best defenses," CSO, 2013.

[28] J. Gramage, "Just in Time Research: Data Breaches in Higher Education," EDUCAUSE Louisville, USA.2014.

[29] J. Bolkan, "Education Data Breaches Double in First Half of 2017," Campus Technology, Chatsworth, 2017.

[30] S. E. Chang and C. B. Ho, "Organizational factors to the effectiveness of implementing information security management," *Industrial Management & Data Systems*, vol. Vol. 106, pp. pp. 345-361, 2006.

[31] M. Suter, "Information security surveys as instrument of risk analysis " *European CIIP Newsletter*, vol. 2, pp. 22-24, 2006.