Managing Students' Academic Information: How Are Public Higher Education Institutions In Uganda Prepared To Deal With Internal Cyber-Attacks?

Mary Basaasa Muhenda
Uganda Management Institute

Abstract

Information systems in developed and developing countries have been equally threatened by cyber-attacks which are deliberate exploitations of computer systems, technology dependent enterprises and networks that can compromise data and lead to cybercrimes like information and identity theft. The study established the magnitude of cyber-attacks in Public Higher Education Institutions (HEIs) in Uganda by insiders likely to access vital information. Investigations into the likely causes of internal cyber-attacks and the level of preparedness on the part of Public HEIs to counteract any cyber threats associated with internal staff or trusted vendors were undertaken. A self-administered questionnaire and an interview guide were developed to solicit respondents' views on whether 1) internal cyber-security threats are a reality 2) the magnitude of cyber attacks in Public Higher Education Institutions in Uganda 3) the likely causes of internal cyber-security threats and 4) the level of preparedness on the part of Public HEIs to counteract any cyber threats associated with internal staff. Four purposively selected Public Higher Education Institutions that have computerised students' information systems and in recent times suffered loss of students' information were included in the study. Respondents were randomly selected from functional departments' staff lists while key informants were purposively selected from functional departments and their views analyzed both qualitatively and quantitatively. Findings show that cyber-attacks are a real threat and do occur regularly although HEIs are sometimes not forthcoming in reporting their existence for fear of damaging their reputation and credibility. Results indicated lack of user education, unethical conduct, absence of policies, inadequate budget provisions, and cultures not easily adaptable to change, suggesting low levels of information security preparedness in many HEIs. The article provides recommendations including but not limited to: adequate information security budgets, strengthening of information security policies and disaster preparedness strategies which HEI could espouse to avert internal cyber-attacks.

Key words: Cyber-Attacks, Public Higher Education Institutions, Information Security

Introduction

Cyber-attacks have become so insidious and yet many public organizations have not paid much attention due to lack of clear understanding of the phenomenon and or being ill-prepared to deal with both internal and external cyber-attacks. According to Techopedia (2014) a cyber-attack is a deliberate exploitation of computer systems, technology-dependent enterprises and networks whose perpetrators use malicious codes to alter computer codes, logic or data resulting in disruptive consequences that can compromise data and lead to cybercrimes like information and identity theft. If we agree with Hoslp (2005) and Laudon and Laudon (2018), that information is vital to communication and a critical resource for performing work in organizations and whose real or perceived value can be gauged in current or prospective decisions, organisations have to understand the extent and implications of cyber-attacks and the strategies to curtail the repercussions. Unless addressed, such repercussions are likely to influence the confidentiality, integrity and availability of vital information like student records.

Background

Today's organizations are prone to having their Information Systems compromised by both intentional and unintentional acts (Bamrara, Singh & Bhatt, 2013; Helms, Ettkin & Moris, 2000; Smith & Rupp, 2002). Whereas unintentional acts can be easily corrected or avoided through training and supervision, intentional acts may be difficult to detect. Such acts may be due to sabotage intended to destroy, alter information and destroy systems or acts of computer fraud intended to steal data, delete or alter records and files or create false information (Haugen & Selin, 1999). Cyber-attacks have been so rampant in public organisations worldwide and in Uganda specifically. This is not new, as earlier research reported how international universities are prone to loss of intellectual property, sensitive research and personal information, costing universities lots of money and badly damaging their reputation (Hemenway, 2014; Centre for Responsible Enterprise and Trade [CREATe.org, 2017).

There is further evidence from recent surveys from the US on the state of cybercrime in 2013 and from CREATe.org (2016) whose findings confirmed how higher education institutions were more vulnerable to cybercrime, with the majority of cases committed by internal staff. According to Cyberattacks.com (2014), the University of Maryland experienced a data breach affecting 200 students' records as far back as 1998 and that a North Dakota University computer system was also hacked into. The 2016 Center for Responsible Enterprises and Trade report revealed that higher education was more vulnerable to cybercrime, with hacking accounting for 36% of all cybercrime. The report further alleges that in 2015 and 2016, many big universities like Johns Hopkins and University of Central Florida were seriously hit by cyber-attacks. All these are indications that cyber-attacks are a reality in higher education institutions throughout the world.

Against this background, this study investigated the existence of internal cyber-attacks, and the level of preparedness on the part of HEI in as far as potential risks associated with internal cyber-security threats on students' information systems by internal staff are concerned. The study answered the following specific questions:

- Whether internal cyber security attacks are a reality and the level of magnitude in Public Higher Education Institutions in Uganda;
- What are the likely causes of internal cyber security attacks? and
- What is the level of preparedness on the part of Public HEIs to counteract any cyber security attacks associated with internal staff

The Problem

The potential attacks associated with cyber security in particular are a big challenge for higher education institutions in developed and developing countries CREAT 2017 & Hearn, 2017). Higher education institutions in Uganda have not been an exception, as cases of lost marks, theft of information, disclosure, alteration and or destruction motivated by a multitude of reasons such as profits, fraud, mistrust, malice have been reported (Muhenda & Lwanga, 2012; Muhenda, 2014; *New Vision*, 2016; *Daily Monitor*, 2017). In one consultative meeting held in November 2013 at Makerere University and attended by Academic Registrars from Public HEI, members noted that there was frequent unauthorized access to students' databases and data infiltration which, though no concrete evidence could be adduced for fear of loss of the institutions' credibility and reputation, was majorly committed by internal staff. The Vice Chancellor of Makerere University is also reported to have hinted on change of marks in the Results Management System, internal staff being the major culprits (Independent Magazine 2017; Mukhaye, 2017). Unless the challenges are addressed, HEI are likely to experience data infiltration, reputational implications and all forms of liability like threats to national security and loss of credibility. Techopedia (2014) also cites common consequences arising from cyber-attacks that include but are not limited to: identity theft, fraud, spamming, trojans and viruses, stolen hardware such as laptops or mobile devises, denial of service attacks, breach of access, system infiltration, website defacement, instant messaging abuse and unauthorized access that could also affect HEIs in Uganda.

Review of Related Literature

Managing information involves coping with a myriad of information sources and ultimately making decisions about what to do with it. Managing information is important to an organization because it allows for increased knowledge, decreased inefficiency, and better creation and implementation of action plans to address areas of opportunity (Helms, Ettkin & Morris, 2000; Wood-Harper, 1998). The value of information in organisations is related to better decision making that results in actions which enable managers to propel the competitive stance of their organisations, solve problems and improve business by generating more revenue to support organisations' objectives. This therefore necessitates some system which Knight and Silk (1990) and Laudon and Laudon (2018) refer to as an information system (IS). IS should facilitate information flow into, within and outside the organisation and provide structures for the management of information so that information can flow to the right recipients in right quantities at the lowest possible costs for effective decision making. However, organisations' reliance on technology and the delicate software and hardware architectures have created widespread opportunities for theft, fraud and other forms of computer crimes by outside and inside offenders in private and public organisations (Bamrara, Singh & Bhatt, 2013).

Bologne (1993), as quoted by Hengen and Selin (1999), outlines factors likely to enhance internet fraud including inadequate rewards, inadequate management controls, inadequate feedback mechanisms, lax disciplinary rules and motivational issues. Hengen and Selin (1999) emphasise that management, supervisory laxity and weak internal control systems are likely to perpetuate internal fraud. They observe that effective systems ought to include preventive, detective and corrective controls and that many computer frauds go undetected while the majority of these disasters are never publicly reported for fear of adverse publicity or fear of system weakness disclosure. Though HEIs have made great strides in physically protecting the system components, little has been done to deal with "trusted" employees who have access to the Information System. And as HEI's dependence on ICT grows, risks associated with system compromise also increase and hence the need for this research to establish whether such challenges were similar to those facing higher education institutions in Uganda.

Fore (1997) observes that many people are only concerned with big punks and computer vandals who roam around on the internet looking for the next computer system to break into, forgetting the authorized users who commit unintentional mistakes. According to Fore, cases of system administrators accidentally reformatting their servers' hard drives during their routine backups of the systems and users accidentally overwriting or wiping out valued documents, disfigured operating systems and poorly written programmes can lead to data destruction. Such unintentional mistakes were found to be going on unabated in HEIs hence good justification for our research in Uganda. The mistakes notwithstanding, the use of social media on mobile devices in the workplace has created new security challenges to organizations. More employees are using their mobile devices to access social media sites and yet mobile devices have weaker defense capabilities (He, 2013). According to Miller, Voas and Huribert (2012), the portability of mobile devices makes it easier to have them lost or stolen and that chances of data loss or leakages are much higher compared to PCs or laptops. Many employees access sensitive corporate information with their mobile devices and yet IT departments have little control over such devices (McAffee, 2012). This is confirmed by a survey done by He (2013) which reported that many users developed third party applications with malicious intent on social media sites like face book and twitter. He further posited that cyber criminals have been uploading malicious applications to media sites like face book and that once these malicious applications are accessed and installed they could cause malicious damage. Since many of administrators in Academic departments are registered members of social media and given the dearth of research on internal cyber-attacks in HEI in Uganda, this study was justified.

According to Hengen and Selin (1999), there are many computer system security risks, some of which have never been taken seriously by many public organizations and that manipulation of data and files may be the most difficult to deal with as there are no outward signals that something has gone amiss. Some common vices cited by Hengen and Selin (1999) include alternating or stealing data files often by disgruntled employees; theft or misuse of computer output as in the case of Local Area Networks (LAN) that expose computer-generated output to a larger audience, for example shared printers for ease of access with output sent through interoffice mail is subject to interception. Unauthorized access to systems or networks to hackers taking advantage of the weak security provided for dual-in and remote access facilitated by computer-based fraud techniques like trojan horse, trapdoor, super zap, masquerading, hacking, browsing, viruses, eavesdropping.

Helms, Eltkin and Moris (2000) cite other risks attributed to residual files termed as files that may have been deleted but are still accessible in the system which can easily be extrapolated by hackers. The duo claim that even when operating files are terminated, they can still linger within the confines of the hard drive and could be easily accessed as long as the auto or manual save is executed. The print queue is another source of stored documentation within the hard drive where hackers can link data through the printer queue in order to obtain deleted documents. Helms et al (2000) also hinted on hacking through penetration of internal caches via the hard drive since the internet can store all files, searches, e-mail transmission and graphs into one's internet cache and internet history file. Amidst all these threats, how are HEIs prepared for internal cyber-attacks and what is the magnitude of such threats?

Methodology

The study employed a descriptive cross-sectional survey design that applied qualitative and quantitative approaches to analyse data. The study covered four out of eight purposively selected public institutions, two that have in recent times suffered loss of students' information and two that have computerized their admission and examination processes. Respondents were randomly selected from staff lists in Academic Registrar and Finance Department offices in charge of admissions, registration, processing of examination results, billing and receipting of tuition, ICT departments. In order to limit bias, respondents were picked in such a way that every fifth name on the register was chosen in order to give an equal chance of representation. Key informants who were purposively chosen basing on their relevant knowledge, authority and experience on the subject included Academic Registrars, Faculty Deans, Heads of Department, ICT managers, Contractors and other ICT venders granted legitimate access to such sensitive data and systems.

To ensure goodness of data assessment to determine consistency and that the right variables are measured using the correct measurement, reliability and validity of data instruments were ascertained. The instruments were formulated and pretested in one HEI where a few senior colleagues were requested to critique the instrument after which all comments were incorporated to improve both the face and content validity of the instrument. All items in the questionnaire were critically examined to advise on content, context and conceptual perspectives. Content validity was assessed and the content validity index (CVI) computed at 0.7 which is within acceptable levels, according to Amin (2005).

Corrections were made and discussed with fellow staff and questions were further refined. Interview guides were formulated to obtain detailed data about the studied variables.

Qualitative and quantitative data analysis techniques were adopted to triangulate the data collection methods and to obtain hign quality data. Descriptive statistics were used to meaningfully describe the distribution of scores using a few statistics of mean, percentages and standard deviations especially in analysing background information, respondents' views on particular items and key respondents responses. A qualitative analysis for purposes of capturing respondents' views on beliefs, values, feelings and personal judgement was adopted. Thematic analysis technique was used to analyse qualitative data. The process involved careful reading of all the captured responses with the intention of developing themes based on the meanings of underlying responses. The information was thereafter transcribed verbatim directly from the note books, organized according to the themes and categorized according to the relevant variables of the study to draw balanced conclusions.

Findings

Staff in functional departments in addition to internal trusted staff including employees like staff in teaching Departments, Faculty Deans and Heads of Department, ICT staff, contractors and other venders who are granted legitimate access to such sensitive data and systems were part of the study.

Respondents' Profiles

The 64 employees who took part in the study offer the following profile. Thirty nine per cent (39%) of the respondents were female while 61% of the respondents were male, an indication that the majority of staff interviewed were female. The administrative staff handling students' records made up 45% of the respondents, 20% were teaching staff, 13% were support staff, Heads of Department and University Officers were 11% and only 3% were vendors -- an indication that all stakeholders were fairly represented in the sample size. Twenty-three per cent (23%) worked in the Academic Registrar's departments, 13% worked in the Finance Department, 11% worked with the Information Technology Departments, 8% worked at School and or Faculty levels, 8% of staff worked for the Heads of Department, 5% worked with Higher Degrees Departments and only 3% worked for Distance Learning Centres and or Outreach Centres. Of those interviewed, twenty-seven per cent (27%) have been employed for 7-9 years, 25% have been employed for 1-3 years, 23% have been employed for 4-6 years, 20% have been employed for over 9 years and only 5% have been employed for less than one year. Results of respondents' education background showed that 34% hold Master's degrees, 25% hold Bachelor's degrees, 20% hold Ordinary Diplomas, 16% hold Postgraduate Diplomas while 3% hold Doctoral degrees, which distribution is a fairly good representation of respondents with different educational backgrounds. .

The section below presents the findings from the self-administered questionnaire and from key informants arranged in sub-themes that emerged from recurring patterns of responses:

Accessing information from the web

The majority of respondents (58%) agreed that documents pertaining to students' data are posted on the universities' websites. Fifty-five per cent (55%) claimed that similar documents are archived and conserved online, while sixty one per cent (61%) claimed that most of the information about students' profiles can be accessed online. Without their supervisors' consent or knowledge some staff, especially administrative officers, intimated that they actually do cloud computing and save in drop boxes. With more than 50% of the respondents confirming the availability of students' data online, chances of cyber attackers accessing such vital data are likely to be real and could increase. Some IT staff in public HEIs in Uganda use internet forums to ask industry colleagues for help in fixing computer system failures, which can provide hackers more valuable claims about an Institutions network. These trends are a pointer to serious threats arising from recent vulnerabilities that come with social collaboration, use of mobile devices, storing vital information in the cloud and digitizing sensitive information, among other threats.

Over-reliance on vendor or donor-based software

One lead team member intimated how his university has challenges with using a wrong software model that was donated by funders. He cited how consistent activation of modules exposed the system to many "intruders" during the course of customizing the software. During the interviews, it was intimated that a few universities had accessed vendor-driven software and that many systems developers would frequently access their information systems which was likely to compromise their information security and exposed their organisations to possible cyber attacks. With this kind of reliance on outsiders, it would be difficult for any HEI to prepare adequately for possible cyber attacks when the Institution is not in total control of their information system.

Exposing Data as a Result of Stolen Hardware

Although some staff had lost mobile phones, the majority did not think it had anything to do with people aiming to access official information. It was actually found out that those stolen were not smart phones and therefore the chances of people using them to access vital information was ruled out. However, one senior officer intimated that because of police blocking stolen mobile devices expeditiously and following the recent rigour in registration of all mobile phone devices, internal attackers may not find this as a viable alternative. Two HEI reported loss of computers in the Academic Registrars Departments during examination periods where two of the stolen computers in one HEI was used for processing examination results. When asked about the level of preparedness to this effect, staff referred the interviewer to the ICT Manager and Deputy registrar in charge of ICT.

Use of Mobile Devices

Many ICT staff said that they do use their mobile devices to store official information though all ICT managers interviewed said that this is not an official policy. However, one ICT manager regretted his inability to restrict staff from using personal mobile devices to conduct official business because of their vulnerability and because they have a heavy toll on the official bandwidth. The majority of ICT staff agreed that mobile devices are a big threat to information security though nothing much had been done to curb their utilization. All these revelations point to inadequate preparedness for probable cyber attacks and insufficient information security policies and procedures.

One staff member Academic Registrars Department intimated that she and her colleagues use their personal mobile devices to undertake critical activities like admissions and or registration. When asked as to whether she had thought about the possible security threats, she responded as follows; "Oh my God, it had never crossed my mind that anybody could use my device to alter marks or tamper with my official information, this is an eye opener for me and my colleagues”.

Limited Use of Antivirus

When asked whether HEIs install, upgrade and regularly update antivirus as a way of minimising cyber attacks, less than fifty per cent (46%) of the respondents said that their universities are compliant. In a lengthy interview in one HEI, one ICT Manager confided in the interviewer that because of budget constraints, regular purchases and or updates of antivirus software was not always a priority to those responsible for drawing budgets. In yet another university, an ICT Manager had this to say, "Our antivirus had expired more than six months ago and my constant pleas have been fruitless."

All these findings are an indication that some HEIs may not be prepared in an unlikely event that a cyber-attack disaster occurred.

Unauthorized Access

More than sixty per cent (60%) respondents agreed that there is a likelihood of authorized access to students' data. Some few data clerks narrated how they sometimes receive promptings that their files are being accessed from another location, an indication that either some internal or external persons could have access to the information. In one particular university, more than six data entrants said such incidents are usually rampant during examination periods. When asked whether they were likely to be external, the majority suggested that it was likely to be an internal job; and they pointed fingers at staff in ICT Departments.

Insufficient Security Training Awareness

Only thirty-four per cent (34%) of the respondents agreed that there exist training opportunities on information security for staff handling records. Further probing however, revealed that only forty-six per cent (46%) of staff had been sensitized on the importance of information security. Some ICT staff said that they had never had serious training on security awareness though a few managers had attended some training which they said was not adequate given the kind of levels that security attacks have reached. Some few ICT managers who had attended some training had not shared what they learnt; and for those who attempted to share with some staff, it was not systematically done. They intended to run sensitisation seminars. The low percentage of trained personnel points to a serious problem of lack of security awareness among staff handling students' records. And one key informant observed, "Some people are ignorant of dangers that are presented by computers". This needless to say, is an indication of lack of preparedness on the part of public HEIs.

Sharing passwords

The majority of staff handling students' records (79%) claimed that they share their passwords with colleagues while fifty per cent (50%) admitted to giving ICT technicians their passwords. All these responses point to lack of security consciousness' on the part of HEI which internal people could exploit. One ICT manager reported that sometimes staff are prompted by the computers to change passwords and this minimizes forced entries in "people's privacy". At least in three HEIs, these promptings were a common occurrence and an indication of some level of security consciousness on the part of HEI.

Inability to log off and turn off computers

Majority of staff handling students' records in HEIs (83%) admitted that they do not turn off their computers when they finish working for the day whereas seventy four (74%) do not log off their computers when moving from their work stations. These revelations point to the possibility of aspiring cyber attackers having easy access to staff documents; and when probed further, three respondents said that they have never thought of any possibility of their actions as a loophole for cyber-attacks an indication of lack of preparedness to handle possible cyber attacks

Uncontrolled Social Networks Membership

More than half of the respondents agreed that they belong to a number of social networks and more than forty per cent (40%) intimated that they search for and download updates and programmes quite often, which actions are likely to compromise information security. When probed as to whether they have ever thought that this could be a security threat, the majority were non-committal and feigned ignorance of the security implications. Some data entry clerks admitted to using their smart phones to download personal data from different social platforms and sometimes using institutions' connectivity to access the internet. This confirmed lack of security awareness, and unless HEIs educate their staff more on possible security threats, the risks are likely be overwhelming.

Inadequate Information Security Audits

Staff lack skills and tools, according to one ICT manager who said: "Recently Auditors carried out an audit but it wasn't thorough because they are IT handicapped, and what they did was not comprehensive as it should have been".

He cited absence of ICT Audit tools and mentioned that, for instance, in the Finance Department, rights are periodically revisited with the agreement of the HEI's Bursar who incidentally was not well grilled in matters of cyber security threats. In an interview with Audit Committee members in a participating HEI, members decried lack of skills on the part of HEI auditors to carry out ICT systems audits and fewer systems expert external auditors who could help institutions to undertake such specialised audits. Scanty audits coupled with absence of system audit experts point to lack of preparedness on the part of HEIs in Uganda and a security risk to HEIs information sources.

Unsatisfactory Incident Monitoring

Results showed that incident monitoring is not diligently enforced in most HEIs. One ICT desk help officer said,

> Ideally the server and client are expected to record incidents but because these two record very detailed processes it is very difficult to fish out the security incidences. I propose that a plug-in could be bought and installed so that it beams those incidences that amount to security threats so that they are attended too quickly. ICT Help Dest Officer

Another ICT manager expressed his disappointment and intimated to the interviewer,

> Previously, staff would call and report a fault. I have instituted log books where all faults and problems are recorded. Staffs are assigned what to do following the log books and at the end of the day staffs are expected to record updates of what has

> transpired but unfortunately, many have not done so. (ICT Manager).

The majority of ICT staff in HEIs had not embraced this fully though they were all aware of the importance of incident monitoring. All these revelations point to inadequate preparedness on the part of HEIs. However, one lead person in an Institution that had the students' application and registration processes fully computerised said that his Institution does not take chances and confirmed regular incident monitoring.

Inadequate Budget Provisions

Almost all participating HEIs cited insufficient funds as the greatest contributor to cyber threats. They attributed lack of funds to buy antivirus kits, insufficient funds to train both staff and managers and purchase computing equipment, network infrastructure and human resource procurement to lack of funds to tighten information security measures. Some ICT managers claimed that ignorance on the part of senior managers coupled with poverty were the most serious setbacks impacting heavily on HEI security endeavours.

Lack and or Scanty Policies and Procedures

Staff narrated how there are no policies to mitigate the information security risks associated with mobile devices, social media and cloud computing. Surprisingly, even in those institutions that had policies, most staff were not very conversant with their policies. This even applied to senior staff like some Academic Registrars, University Bursars and Deans of Schools who were totally ignorant of existing policies. This left the researchers wondering as to how prepared HEIs were. Almost all the respondents cited inadequate and or absence of policies as the greatest challenge likely to affect information system security. One HEI that had its admission and registration fully computerized did not have any single ICT policy save for a few administrative notices which by nature are likely to be violated without any serious consequences.

Unethical Staff

Many respondents strongly believed that a good number of staff in ICT Departments, Academic Registrar, Finance and Teaching Departments exhibited corrupt tendencies and could have infiltrated information systems for personal gain. In one HEI that was seriously hit by tuition fraud, researchers heard how internal staff could hack in the systems to either alter students' marks or change records pertaining to students' tuition. Discussions with majority of respondents pointed to unethical staff as one of the major causes of cyber-attacks and were not sure how HEI were managing the issue of ethics and integrity.

Lack of Support from the Executive and Lines of Business

Over 60% of the respondents cited lack of support especially from top and line managers attributable to either an under estimation of cyber attacks' ramifications and or obliviousness of information security matters. Other respondents attributed some managers' attitude to perceived loss for personal gain for those who could have been benefitting either directly or been benefiting as abettors from the information security lapses.

Discussion

The majority (89 %) of the respondents other than the ICT staff admitted that the existence of cyber attacks in public HEIs in Uganda are committed by mainly trusted internal employees and or service providers. Though this study could not predict with accuracy the extent of the problem, findings confirm that it is indeed a big problem facing HEIs in Uganda; though the majority do not want to overblow it due to the sensitivity of students' data, especially information concerning examinations. This finding was also reported by Hemenway (2014) who reported universities' reluctance to disclose their compromised information systems for fear of losing their reputation.

The likely causes of security attacks by internal people are many worldwide but, as outlined in section four, those affecting HEIs in Uganda include but are not limited to the following: accessing information from the web; exposing data as a result of stolen hardware; limited use of antivirus; unauthorized access; insufficient training in ICT security awareness; sharing passwords; inability to log off and turn off computers after work; uncontrolled membership to social networks; inadequate information security audits; unsatisfactory incident monitoring; inadequate budget provisions; absence and or scanty information security policies; and, limited support from executives and peers.

Judging from the responses, it may be concluded that almost all public HEIs in Uganda are not adequately prepared for cyber attacks that are likely to be committed by internal staff. This conclusion is drawn from the responses that seemed to suggest unawareness of the existence and the adverse consequences of cyber-attacks by internal staff, inadequate resources, partial preparedness and slackness on the part of HEIs executive and line managers.

Conclusion

The potential attacks associated with cyber security are a big challenge for public organisations in Uganda and Higher Education Institutions have not been an exception. Earlier research reported how universities are prone to loss of intellectual property, sensitive research, and personal information, costing the universities lots of money and badly damaging their reputation, though many of these studies focused mainly on outside institutions. The findings confirmed internal cyber-attacks as a major challenge facing HEIs in Uganda and the recommendations could be upheld to help administrators to mitigate the vice and attain high levels of preparedness.

Recommendations

- Prohibiting and or regulating staff from using popular services like drop box to store or transfer students' information;
- User education and training on matters of information security and possible threats of internal attacks are a must. Such training will help employees to raise their security

awareness and tread cautiously. According to He (2013), organisations need to raise their employees security awareness on issues of identifying potentially malicious social applications, how to use strong passwords and how to protect data on their smart phones and other mobile devices;

- Initiating general information security policies and in particular policies on social networks, cloud computing and use of mobile devices are crucial;
- Streamlining and or developing incident notification guidelines ought to be embraced by all HEIs in Uganda;
- Adequate budget provisions for purchasing hardware and software, remunerating and training all staff handling students' records, funds for training auditors who audit IT systems and for ICT managers on the latest security threats. Sufficient funds are also required to secure virus protection kits and regularly update them, in addition to hiring security experts to advise regularly and ensure compliance;
- Close scrutiny of new employees and vetting all staff in ICT Departments and Academic Registrars' offices could help HEIs in Uganda to recruit staff of high integrity which could minimise internal cyber attacks;
- Tightening levels of authorization is also strongly recommended with the majority of staff accessing information without obtaining access rights to vital students' records and finally
- Encouraging intense innovations by using internal staff and students who have been vetted and who could develop novice ideas without opening the system to many outside vendors.

References

Bamrara, A., Singh,G. & Bhatt, M. (2013). Cyber attacks and defense strategies in India: An Empirical Assessment of Banking Sector. *International Journal of Cyber Criminology*, *7*(1), 49-61.

Bell, S. & Wood-Harper,T.(1998). *Rapid information systems development*, 2nd Edition. London. McGraw Hill.

Editor. (2017). Editorial. *Daily Monitor Newspaper*, Kampala, Uganda. Retrieved from www.monitor.co.ug

Editor. (2016). Editorial. *New Vision Newspaper*. Kampala, Uganda. Retrieved from www.newvision.co.ug

Editor. (March 2017). Makerere University under investigation over academic fraud. *Independent Observer.* Retrieved from www.observer.ug

Hearn, T. (2016). *University Challenge: cyber-attacks in higher education*. Downloaded from www.vmware.com

Hegen, S. & Selin, J. R., (1999). Identifying and controlling computer crime and employee fraud. *Industrial Management & Data Systems, 99*(8), 340 – 344.

Helms, M. M., Ettkin, L.P., & Morris, D.J. (2000). Shielding your company against information compromise. *Information Management & Computer Security, 8*(3), 117 – 130.

Hemenway, C. (2014). *The price of collaborating environments at Universities.* Downloaded from http://cyberattacks .com.

Kyakulumbye, S. & Muhenda, M. (2013). *Integration of ICT in improving Local Government service delivery: An evaluation of ICT intervention value for money*. [Conference Presentation] Commonwealth Research Conference in Uganda on May 13, 2013.

Laudon, K.C. & Laudon,J.P. (2018). *Management information system: new approaches to organization and technology*. Prentice Hall International Inc: New Jersey.

Miller, K.W., Voas, J. and Hurburt, G.F. (2012). “BYOD” security and privacy considerations. *IT Professional, 14*(5), 53-55.

Muhenda, M.B. & Lwanga, K.E. (2012). Managing records in higher education institution in Uganda: can human resource policies savage the situation. *World Journal of social sciences*, *2*(2), 74-83.

Muhenda, M.B. (2014). *Information systems in public organisations in Uganda: how are Higher Education Institutions prepared to deal with internal cyber-attacks?* [Conference Presentation] IIAS conference, Morocco, June 2014.

Patterson, H. (2013). *Investigating internal network attacks.* Downloaded from www.extremnetworks.com.

Smith, A.D., & Rupp, W.P. (2002). Issues in cyber security: Understanding the potential risks associated with hackers/crackers.
Information Management & Computer Security, 10(4), 178 – 183.

Techopedia. (2014). *Cyber attacks definition*. Downloaded from www.techopedia.com.

Trim, P. R. J. (2005). Managing Computer security issues: preventing and handling future threats and disasters. *Disaster Prevention & Management*, *14*(4), 493 – 505.

Wu He. (2013). A survey of security risks of mobile social media through blog mining and extensive literature search. *Information Management & Computer Security*. *21*(5), 381 – 400.

Zalaznick, M. (2013). *Cyber attacks on the rise in higher education.* Downloaded from www.universitybusiness.com