IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Adoption of Physical Security for Information Systems in Universities in Kenya

Rongo University
School of Science Technology and Engineering
Department of Mathematics, Statistics and Computer Science

Authors:
Ms Jane Akello Juma (1)
Dr. Charles Ochieng' Oguk, PhD (2)

Abstract

Information systems are increasingly becoming important facilitators of efficiency in academic and administrative services' delivery in universities world-wide as well as in Kenya. To meet the requirements of confidentiality, availability and integrity of the information systems, universities need to ensure physical security of these systems. This study specifically investigated the implementation levels of physical security measures employed by the randomly sampled private and public universities in Kenya. Questionnaires were used to collect data from purposively sampled university staff members, the data was then analyzed, interpreted and presented using both qualitative and quantitative methods. Data was analyzed to yield frequencies which were expressed into percentages for better understanding. Results revealed that while physical security mesures for information facilities are employed by a lot of the universities, most vital aspects like signage implemetation, ICT asset register, and recovery of portable devices is widely not practiced. The paper recommends better implemetation of physical security safeguards for university information systems. Further emanating research areas from the research study are discussed.

Keywords: University Information Systems, Physical security measures, operation areas, IT Security.

Introduction

Universities have increasingly continued to automate their operations. Considering Information systems are at the heart of automation, any neglect of physical security of information systems is unfortunate and may lead to significant consequences, (Njoroge, Wambiri, & Ogeta, 2015). While many universities in Kenya have suffered IT security incidents which compromise confidentiality, integrity and availability of information systems (Okibo & Ochiche, 2014), most of the cases go unreported (Gesare, Michael, & Odongo, 2016). According t Helsloot, Tillem, and Erkin (2017), universities use both hardware and software computer facilities whose security levels in the surrounding environments should be considered.

The facilities are kept safe in some forms of physical facilities for security provision such as metallic grills, perimeter fences and locked server – rooms (Arnaud, Cortier, & Wiedling, 2013). The study showed in many cases that universities' information systems have been rendered unavailable by disconnected network cables, hardware theft, and system vandalism. Newswire (2018) highlights that availability of information systems' resources in Universities in Kenya is affected not only by hacker activities, but also by physical security incidents like natural disasters, accidental and deliberate actions including but not limited to disconnection of network cables, computer theft, vandalism, floods, sabotage, fire, strikes / riots and lighting. Whenever the physical security systems are breached, the incidents expose information systems of universities to high level risks of data loss and compromised content integrity.

In Kenya, since the year 2012, a public university has experienced more than three incidents of both internal and external cuts on fiber- optics lines, which rendered the entire information systems unavailable for users. In the year 2014, inter-block fiber optics cable linking the university's server – room and office of the registrar- academics was accidentally cut by laborers when weeding street flowers along the area which was traversed by optical fiber back-bone underneath. This incident made the university server that was hosting students' data to be unreachable, thus unavailable for the affected department for weeks, (Oguk, 2016). It was noted that there was no signage identifying the areas traversed by data lines within the university. In a separet incidence, the university reportedly lost two desktops from the students' computer lab in the year 2013. The hardware loss was attributed to uncontrolled physical access to ICT premises. In November of the same year, another public university's IT system was struck by lightning, compromising information system's availability.

These experiences concur with (Njoroge et al., 2015), which reviewed information systems, and concluded that physical security is a crucial element worth considering in systems' security management. The studies stress the need for incorporating physical security features in the development of IT security metrics, to show the levels of physical interventions and practices adopted in an organization for IT security management. The highlighted KPIs constitute the building blocks for physical security as an element of IT security in the metrics model.

Statement of the problem

While studies concur that physical security of information systems is paramount, a lot of the existing studies hardly focus on the adoption of physical security safeguards in the entire universities' information systems. Some studies like Njoroge et al., (2015) only focused on the physical security measures in computer based information systems in the library. If this is not addressed, the information gap on the levels of implementation of physical security around universities' entire information systems will continue to exist.

The Objective

This study aimed at investigating the adoption of physical security protection for information systems' facilities in universities in Kenya

Review of related Literature

Li, Sui, Chi, and Chen, (2016) defined information systems' physical security as the protection of information systems: personnel (users), hardware, software, data and networks facilities from physical threats, actions and events, including flood, fire, natural theft, burglary, disasters, vandalism and even terrorism that may cause loss or damage to the information systems.

Global trends have shown concerns about computers systems' physical security. In Uganda, proper physical control barring unauthorized entry into server rooms was found to be a remedy for malware menace (Solomon, 2017). In Kenya, (Okibo & Ochiche, 2014) investigated the challenges facing information systems security management within private universities, and highlighted computer theft, inadequate physical security, sabotage through cable cuts and system vandalism, among the key challenges affecting information system security management in most Kenyan institutions of higher learning. The study found that even though physical security practices are overriding other elements of IT security, most universities only consider minimal physical interventions around information assets. However, the few universities which adopt physical security to any levels hardly employ relevant standards as bench-marks for physical security implementation in the universities.

The necessity of physical interventions around IT facilities is supported by (*Cyber Physical Systems (CPSs)*, 2015) which highlighted that the availability of information systems' resources in universities is affected not only by hacker activities, but also by physical security incidents like natural disasters, accidental and deliberate actions, including disconnection of network cables, computer theft, vandalism, floods, sabotage, fire, strikes/riots and lighting. The studies pointed many cases where universities' systems' unavailability has been occasioned by disconnected network cables and compromised physical security of information systems.

In a research conducted within a private university based in Nairobi - Kenya (Nyamongo, 2012), the findings concurred with the findings of (Bichanga and Obara, 2014) on the challenges facing information technology security in the universities. Specifically, it cited poor policies on physical security controls and unfocused IT security frameworks. It claimed that the current IT security implementation frameworks are not comprehensive enough, as they are lacking in content of physical security. As a result of this, Nyamongo proposed a better IT security management framework which stresses the need for physical barriers around the server rooms as well as signage along critical data lines. It therefore suggested the need for a further research to explore the incorporation of IT physical security element in portraying the status of IT security in a university.

In summary, physical security as an element of IT security involves the protection of information systems against physical threats that may cause loss and damage to information systems. The foregoing studies indicate that loss and damage to information assets occur within universities in Kenya and beyond, yet not all universities take physical security interventions as a matter of priority. Also, in the few universities where physical security is adopted, relevant standards are hardly considered. The studies concur that physical security is so important in IT security that it should constitute a framework for IT security management.

Reserch study gap

There is a gap of literature in that, while information systems' physical security is paramount, the foregoing studies hardly focused on the levels of implementation of physical security around the entire university information systems' facilities. It is in this light that this study focused on investigating the levels of implementation of physical security safeguards in the selected public and private universities in Kenya.

Theory of Planned Behavior (TPB)

This theory is among the theories for ICT systems' implementation and adoption. According to Armitage and Conner (2001), the theory is among the most influential theories that inform models for information security management in business and organizations. Ajzen (1991) presented the theoretical model - (TPB), which focuses mainly on cognitive self-regulation but takes into account an additional construct of perceived behavioral control. According to Ajzen (1991), perceived behavioral control is the perception of control over the performance and manifestation of a given behavior. This explains the behavioral patterns of IT systems' users and administrators together with how the behaviors affect implementation of physical security for information systems

Taylor and Todd (1995) studies concur with Mathieson (1991), as they separately analyzed Theory of Planned Behavior, especially focusing on cognitive self-regulation and taking into account an additional construct of perceived behavioral control. Both researchers concluded that it can influence behavior of people and predict an individual's intention to use the guidelines of information and communication systems - ICT. This theory applies to the current study as it can be used to focus on cognitive self-regulation and perceived behavioral control to influence the users and information systems administrators in adopting practices that enhance information security within universities in Kenya. The basis of the theory of planned behavior is that attitudes together with perceived control and norms, to a great extent, do predict peoples' intentions. The intentions are used to predict deliberate and planned behavior - which are the practices that enhance information security. According to the theory, intention is determined by three things: attitude, perceived control, and subjective norms. Information security managers can thus work on the three factors to direct intentions of users towards information security practices.

Research Methodology

The following research methodology was employed.

Research Design

Exploratory research design was applied in this study since there was need for first hand understanding of the physical safeguards employed to secure university information systems in Kenya, being that the topic is relatively new and very little had been documented on this spectrum.

Population

The target population for this research included the product of thirteen 13 section heads: as backed by studies and the seventy (70) universities in Kenya according to CUE in the year 2015, thus a population of (13x70=) 910 users and administrators in the universities.

Sampling

Mixed sapling approach was adopted in this study. First, stratified sampling which aimed at categorizing universities as public and private was used. Secondly, ten (10) percent random sampling was further employed on each strata to yield a total of seven (7) universities as shown on the table below.

The university population and the sample

	Stratified Sampling	Simple-Random Sampling
Public universities	33	3
Private universities	37	4
Total	70	7

Purposive Sample sampling

Operation Area (Category)	**No of team leader(s)**	**No of universities**	**Sample size per category**
IT leadership	1	7	7
Systems administration	1	7	7
Network administration	1	7	7
Security administration	1	7	7
DB administration	1	7	7
Students' finance	1	7	7
Students registration	1	7	7
Examinations	1	7	7
human resources	1	7	7
Internal Audit	1	7	7
Library	1	7	7
Computer Laboratory	1	7	7
Students Leadership	1	7	7
Totals	**13**	**(13X7)**	**91**

Data collection instruments

Data was collected using well designed questionnaires and this was supplemented with direct observations to ensure quality.

Data analysis and interpretation

Both qualitative and quantitative analyses were employed. Data was analyzed using SPSS software and Microsoft Excel to yield pertinent statistical values addressing the objective of the study. Data was analyzed qualitatively whereas respondents' views on implementation levels of physical security safeguards were rated on their effectiveness. On quantitative basis, data was analyzed on frequency-based percentage levels of implementing the physical safeguards. Data was mostly presented in a tabular format.

Results

Implementation of Physical security for information systems

Physical security	**Percentage**
Effective signage implementation	32
systems asset register	48
control access to physical facilities	40
Monitoring of physical facilities	26

This study found that only 32 percent of the universities implement signage effectively, while 68 percent did not, yet, signage implementation along key data lines and computing facilities is very important for ensuring information system security. 48 percent of the universities do effectively maintain IT systems asset register, while 52 percent do not maintain it effectively. 60 percent of the universities do not effectively control access to physical facilities hosting IT systems, while only 40 percent control the physical effectively. The study also found that 76 percent of the respondents agreed that the security of physical computing facilities are not effectively monitored through closed circuit television -CCTV, while only 26 percent of the universities, mainly the private universities do it effectively. This finding concurs with (Njoroge et al., 2015) study which found that out of four university libraries sampled, only one library had implemented CCTV for monitoring the computer based library information systems.

Further, these results concur with Casey (2011), which showed that security levels in the environment surrounding computing facilities ought to be considered in universities. According to Casey, IT facilities are kept in some forms of physical enclosures for security provision. These enclosures include behind the grills, perimeter fences and locked server - rooms, (Stallings & Brown 2008). Further, in support of these findings, Mantic and Simon (2011) considered information systems and concluded that physical security of computing tools is a crucial element of IT security. Moreover, he study's findings support Mangier and Andrew (2014), which highlighted that availability of information systems' resources in Universities in Kenya is affected not only by hacker activities, but also by physical security incidents like natural disasters, accidental and deliberate actions including: disconnection of network cables, computer theft, vandalism, floods, sabotage, fire, strikes/riots and lighting.

Discussion

This study found that physical security plays a major role in IT security management within universities in Kenya. Signage helps to avoid accidental breakage of data communication lines in the university. However, only 32 percent of the universities studied implemented signage effectively, while over 68 percent. Furthermore, 48 percent of the universities do effectively maintain IT systems asset register, while 52 percent do not maintain it effectively. This is despite the fact that any asset register is like an inventory that is paramount in ensuring the availability of facilities. Controlling physical access to sensitive areas hosting computer systems is necessary, yet the study found that 60 percent of the universities do not effectively control access to physical facilities hosting IT systems. On monitoring ICT facilities, the study found that 76 percent of the respondents agreed that the securities of physical computing facilities are not effectively monitored through closed circuit television-CCTV. This is despite the need to do so.

Research Contribution

Inadequate empirical research existed on physical security measures put in place by universities in Kenya to safeguard information systems. This research has highlighted what ought to be done as well as what is being done in the perspective of physical security safeguards in the universities in Kenya.

Conclusion

In conclusion, university computer systems can be safeguarded by adopting the highlighted physical security measures to reduce vulnerabilities associated with various threats such as line breakage, theft and vandalism. They are recommended to adopt these safeguard measures.

Further research is recommended on the major reasons why many universities have not adopted the necessary physical security safeguards in their operations.

References

Arnaud, M., Cortier, V., & Wiedling, C. (2013). Analysis of an electronic boardroom voting system. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. https://doi.org/10.1007/978-3-642-39185-9_7

Bichanga, O. W., & Obara, O. B. (2014). Challenges Facing Information Systems Security Management in Higher Learning Institutions: A Case Study of the Catholic University of Eastern Africa-Kenya. *International Journal of Management Excellence*, *3*(1), 336-349.

Bishop, M. (2003). What is computer security?. *IEEE Security & Privacy*, *1*(1), 67-69.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic press.

Cyber Physical Systems (CPSs). (2015). https://doi.org/10.4018/978-1-4666-7312-0.ch001

Gesare, M. R., Michael, N., & Odongo, A. J. (2016). Influence of Internal Control Systems on Fraud Risk Management among Commercial Banks in Kisii Town, Kenya. *IOSR Journal of Business and Management*. https://doi.org/10.9790/487X-1804032834

Helsloot, L. J., Tillem, G., & Erkin, Z. (2017). AHEad: Privacy-preserving online behavioural advertising using homomorphic encryption. *2017 IEEE Workshop on Information Forensics and Security, WIFS 2017*. https://doi.org/10.1109/WIFS.2017.8267662

Li, J., Sui, Q., Chi, M., & Chen, J. (2016). Design of a chip destructible hardware Trojan. *Proceedings - 2016 IEEE*

International Symposium on Computer, Consumer and Control, IS3C 2016. https://doi.org/10.1109/IS3C.2016.167

Mingaine, L. (2013). Skill challenges in adoption and use of ICT in public secondary schools, Kenya. *International Journal of Humanities and Social Science*, *3*(13), 61-72.

Mong'eri, M. K. (2014). *Security in health workforce information systems: a case of regulatory human resource information system* (Doctoral dissertation, University of Nairobi).

Newswire, P. R. (2018). The Private LTE & 5G Network Ecosystem: 2018 - 2030 - Opportunities, Challenges, Strategies, Industry Verticals & Forecasts. *LON-REPORTBUYER*.

Ndung'u, P. W., & Kyalo, J. K. (2015). An evaluation of enterprise resource planning systems implementation experiences for selected Public Universities in Kenya.

Njoroge, R. W., Wambiri, D. M., & Ogeta, N. (2015). Physical security measures for computer-based information systems: A case study of selected academic libraries in Kenya. *2015 IST-Africa Conference, IST-Africa 2015*. https://doi.org/10.1109/ISTAFRICA.2015.7190590

Nyamongo, D. M. (2012). *Information systems security management* (Doctoral dissertation, Strathmore University).

Oguk, O. C. (2016). Review on Mobile Network Security Issues and Challenges. *Mara*.

Okibo, B. W., & Ochiche, O. B. (2014). Challenges Facing Information Systems Security Management in Higher Learning Institutions: A Case Study of the Catholic University of Eastern Africa - Kenya. *International Journal of Management Excellence*. https://doi.org/10.17722/ijme.v3i1.133

Solomon, R. (2017). Electronic protests: Hacktivism as a form of protest in Uganda. *Computer Law and Security Review*. https://doi.org/10.1016/j.clsr.2017.03.024

Stallings, W., & Tahiliani, M. P. (2014). *Cryptography and network security: principles and practice* (Vol. 6). London: Pearson.

Tarus, J. K., Gichoya, D., & Muumbo, A. (2015). "Challenges of implementing e-learning in Kenya: A case of Kenyan public universities". *The International Review of Researchin Open and Distributed Learning*, 16(1).

Veseli, I. (2011). *Measuring the Effectiveness of Information Security Awareness Program* (Master's thesis).