An Examination of Threats facing Assets in Use in Kenyan Public Universities

Mr. Patrick Macharia Njoroge

* Kenya School of Government, Embu
mashnjoro@yahoo.com

DOI: 10.29322/IJSRP.11.05.2021.p11372
http://dx.doi.org/10.29322/IJSRP.11.05.2021.p11372

Abstract

Globally universities are increasingly dependent on information and communication technology to execute their core operations and functionalities, thus getting exposed to increasing cyber threats and consequently unprecedented security risks. Moreover, Kenyan public universities are not exceptional in using information and communication technology to execute their core operations and functionalities. The study sought to examine the common security threats facing the assets in use in Kenyan public universities. Proper identification and establishment of the security threats facing the universities would inform on the necessary mitigation controls to implement hence effectively mitigate the security risks. The research employed descriptive survey method and was anchored on Operationally Critical Threats, Assets and Vulnerability Evaluation (OCTAVE) framework. The target population was the 31 public chartered universities, which were clustered into two. Simple random sampling was used to select two universities from each cluster while purposive sampling was employed for respondent's selection. Data was analyzed with statistical tools using frequency, percentages, mean, and standard deviation while the results were presented using tables and Likert scale. The study findings revealed that the topmost security threats facing the Kenyan public universities assets were viruses with a mean value of 3.61 out of 5, followed by spam with a mean value of 3.36 and worms with a mean value of 3.10 which were reported to a moderate extent. Hacking attempts attained a mean value of 2.77, while trojan horse had a mean value of 2.62, followed by adware, phishing, denial of service attacks, spyware, spoofing attacks, brute force attacks, ransomware, eavesdropping and SQL injections in that order of prevalence with mean values of 2.59, 2.46, 2.39, 2.33, 2.16, 2.11, 2.10, 2.0, 2.0 respectively. It's evident from the study findings that assets in use in Kenyan public universities are exposed to several security threats and consequently information security risks, which may negatively impact on universities execution of their core operations and functionalities. It's recommended that universities be proactive in implementing necessary mitigation controls to address the security threats they face in accordance with their risk tolerance levels.

Index Terms: Information Security Risk, Threats, Risks, Vulnerabilities, Assets

Introduction

The universities map themselves out as hubs of knowledge generation, preservation and dissemination; and innovation centers (Cloete, Bailey, Pillay, Bunting, & Maassen, 2011). In a bid to fulfil their mandate the universities have been integrating information and communication technology (ICT) into their core operations and functionalities, which includes learning and teaching activities, communication and collaborations, research activities, innovations and developments, and information sharing activities.

However, adoption and use of technology brings with it notable benefits, new opportunities as well as inherent risks (Australian Computer Society, 2016; Andreasson, 2012). The nature of the environment in which the universities operates with open networks and having vast amounts of data, which is available for public access exposes them to various cyber threats and risks, making them vulnerable and key targets for cyber-attacks (Raman, Kabir, Hejazi, & Aggarwal, 2016). The universities' data includes research data, financial data, personal information for both students and university employees, medical and health information, examinations and grading.

Moreover, the universities increased digital reliance to execute their core operations and functionalities, increases their exposure to cyber threats and unprecedented security risks (Business/Higher Education Round Table [BHERT], 2016). The security risks are growing day by day due to the increase in terms of ease, sophistication, automation and frequency of the attacks (BHERT, 2016; Wagstaff & Sottile, 2015; Pandey & Mustafa, 2012). Further, Symantec's threat report on internet security, denoted that 10 percent of all the security threats experienced were affecting the education sector (Symantec, 2015). In the United States, 550 universities were reported to have experienced some form of data breaches between the year 2006 and 2013 (Wagstaff & Sottile, 2015). Further, report by VMware (2016) indicated that over 36 percent of the Universities in the United Kingdom were affected by cyber-attacks on hourly basis and that much of the hacking attacks were targeting the student exam results, intellectual property theft and exfiltration of the research data. Further, according to a report by Raman et al., (2016), there were several universities, which had experienced cyber-attacks leading to compromise of servers and database records, disruption of the functionality of the network, making it unavailable for days, data loss, unauthorized data breaches, and website hacking. A comparative survey by CPS International conducted in 2012 revealed that Kenyan universities were leading in the use of ICT as compared to their counterparts within the East African region (CPS, 2012). A Kenya cyber security report by Serianu (2016), exposed the hacking of the University of Nairobi twitter handle, stealing and leakage of the Ministry of Foreign Affairs data, and web defacement. Teng'o (2017), exposed the rise of cyber-attacks targeting to tamper with the students' academic grades, their fee balances and personal records for both students and employees, in Kenyatta University and Jomo Kenyatta University of Agriculture and Technology (JKUAT). Aineah (2018) reported rampant hacking across a number of local university systems to modify exam grades and generate income by reselling the universities internet connectivity. The Business Daily (2017), reported how Eset East Africa, a security company had won about 750 contracts within a year from clients seeking to have their information systems protected and secured from the increased cyber-attacks in Kenyan private and public sector businesses. These firms include Kenya Methodist University, Britam, Kenyatta University, Nakumatt and Kenya National Bureau of Statistics.

Further, the increase in the cyber-attacks targeting the Kenyan universities ,as well as other organizations both private and public calls for concerted efforts to address the threat to information security (Business Daily, 2017; Serianu, 2016; Teng'o, 2017).Therefore failure to protect the university ICT systems and sensitive data could result in negative aftermaths such as disruption to the functioning of the universities networks and information systems, loss or damage of valuable data, fraud, damage to universities reputation, revenue loss and disruption of critical services once successful attacks are executed. For universities to effectively mitigate the security risks they are facing, they must clearly examine and identify the security threats facing them.

Statement of the Problem

The public universities in Kenya are increasingly dependent on information and communication technology to execute their core operations and functionalities, which is exposing them to increasing cyber threats and hence unprecedented security risks.

Moreover these security risks undermine the integrity, availability and confidentiality of the universities ICT systems, which may impact negatively on the universities ability to execute their core operations and functionalities.

Therefore, the study sought to examine the common security threats facing the assets in use in the universities, which would in turn inform on the necessary mitigation controls to institute to address the existing gaps in security.

Objective of the Study

The specific objective of the study was;

1. To examine the threats facing the assets in use in Kenyan public universities.

Conceptual Framework

The study conceptualized that presence of threats facing the assets in use in the Kenyan universities may impact negatively if actualized thus affecting the universities execution of core operations and functionalities. The relationship is as shown in the figure 1 below;

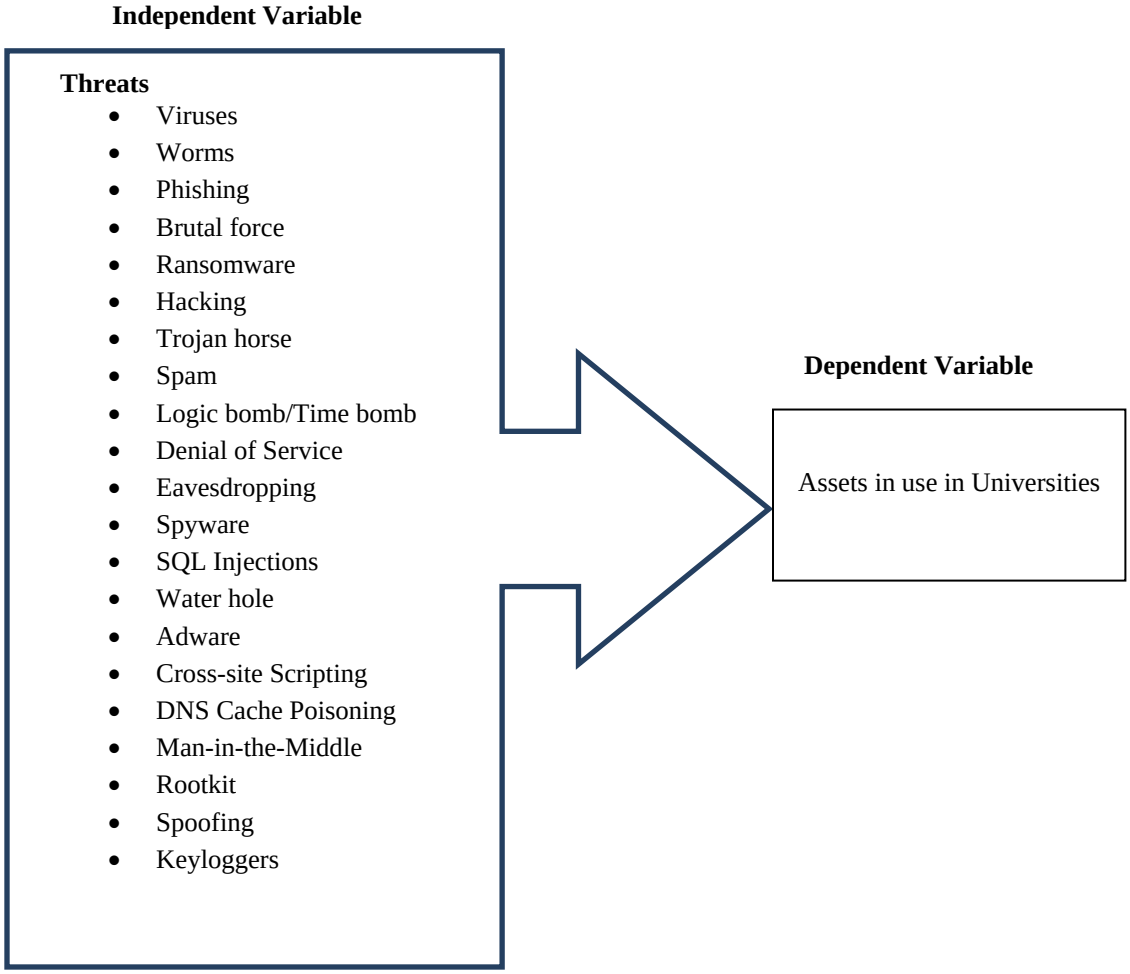

Figure 1; Conceptual Framework
(Source: Authors, 2019)

LITERATURE REVIEW

Information Security Risk Management (ISRM)

ISRM refers to a process whereby the risks, which are associated with the usage of information technology, are managed. ISRM aims to ultimately treat the risks in accordance to the risk tolerance of an organization, since organizations may not be able to fully eliminate risks, but rather attain a risk level, which is acceptable to an organization (Jowi & Abade, 2016). The universities computing environment adopts open networks with vast amounts of data and other resources which support their critical learning and teaching activities, communication and collaborations, research activities and information sharing activities. The students, staff and other stakeholders, must securely access these resources and therefore they must be secured from any vulnerabilities, threats and security breaches (Joshi & Singh, 2016; Raman et al., 2016).

With the threats and vulnerabilities continually evolving, protecting the university's open networks presents key challenges hence the need for risk management (Australian Computer Society, 2016) which is an essential method towards risk mitigation and protection since it requires identification of critical assets, their security requirements, the threats facing the assets and the vulnerabilities and strategies to keep them safe and secure.

Information Security Risks

This are risks associated with the use of information and communication technology. The risks tend to undermine the integrity, availability and confidentiality of the organization's assets.

Assets

In the study, an asset referred to the data, information, business activities and processes, software, hardware and network infrastructure. Alberts and Dorofee (2002) observes that the assets used in the performance of the core operations and functionalities of the universities or organizations are very essential in achieving the mission and the business objectives. Therefore, the assets must be protected from any vulnerabilities, threats and security breaches or incidents, since they can negatively impact on the universities or organizations if they are destroyed or lost, disclosed to people who are not authorized, modified without necessary authorization, or when their accessibility is interrupted.

Threats

A threat is an action, which takes advantage of a security weakness in the system, causing harm to the system or organization (Abomhara & Koien, 2015). Threats always exploit vulnerabilities in the system thus causing loss or harm to an information asset or the organization. The potential harm or loss to the asset is the risk, which needs to be addressed to effectively manage the threats. Since the threats which can negatively impact the universities or other organizations varies widely by size, region and industry, it's incumbent upon the universities or the organizations to understand the risks which they face and therefore institute mechanisms to proactively address them (AON, 2019). Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) requires that universities or implementing organizations establish the threats to their information and related assets which is a key output under OCTAVE criteria, R01.3. The researcher sought to establish to what extent the various threats as identified in literature were affecting the universities. This would assist the universities to identify their risks and hence institute proper mitigation controls for their protection. The threats identified were denial of service (DoS) attack, spam (junk mail), hacking, phishing, structured query language (SQL) injection attack, brute force attack **,** man-in –the-middle- attack, **s**poofing, cross-site scripting, DNS cache poisoning,

eavesdropping, watering hole attack **,** ransomware, adware, spyware , worm , trojan horse, virus , rootkit, time bombs and logic bombs and keyloggers.

Theoretical Frameworks

The study adopted the Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) framework for assessing the information security risks management in the public universities. OCTAVE factors threats, vulnerabilities and assets in its information security risks evaluation thus increasing its accuracy in assessing the risks (Shevchenko et al., 2018; Alberts & Dorofee, 2002; Pandey & Mustafa, 2012). Under the OCTAVE criteria, R01.3 identification of threats to the critical assets is a key output, which goes a long way in informing the risks and mitigation measures to institute. Further, OCTAVE directly contributes to risk management, its well-documented, customizable, leverages on knowledge of people working within the organization, and very flexible, hence well positioned to address information security risks requirements of the public universities in Kenya as compared to other standards such as ISO 27005, ISO 27001, NIST Framework and CCTA (Central Communication and Telecommunication Agency) Risk Analysis and Management Method (CRAMM) (Njoroge, 2020). Through the use of the OCTAVE method, decisions about how to protect the information and the related assets are based on the risks to confidentiality, integrity and availability of the information and related critical assets (Alberts, Dorofee, Stevens, &Woody, 2003), and this enables the organizations to match the protection strategies they employ to the security risks they face, hence addressing the security threats.

METHODOLOGY

The study was carried out in Kenyan public universities. The researcher employed descriptive survey method and qualitative and quantitative data was collected to provide answers to the research questions of the study. The public chartered universities were clustered into two based on their actual year of establishment as fully-fledged universities to ensure equal representation of the universities from the two clusters. A simple random sample of two universities from each of the clusters was selected to give a sample of four universities. The researcher employed purposive sampling to determine the respondents for the survey who were personnel from the information and communication technology and computer science departments of the selected public universities who were well versed with the context of our survey since their daily endeavors revolve around the knowledge domain of the survey The respondents included IT Managers, Systems Administrators, Web Administrators, Network Administrators, ICT Officers, IT Support, Database Administrators, Security Administrators, IT Technologists, Systems Analysts and IT Technicians. The target sample was a 100 respondents from the universities, established after contacting the institutions' heads of ICT departments. Questionnaires were used to collect the primary data of the study while data was analyzed using frequency, percentages, mean, and standard deviation while the results were presented using tables and Likert scale. The instrument of data collection used in the study namely the questionnaire, was developed and subjected to thorough expert review through my supervisors to verify that the instrument measured what it was intended to measure and a pre-test study was carried out.

RESULTS AND DISCUSSION

This presents the results and subsequent discussions

Response Rate

The study targeted 100 respondents, out of which 61 respondents were able to favorably respond, giving a response rate of 61% as clearly tabulated and shown in the Table I**.**

Table I: *Response Rate*

Response Rate	Frequency	Percentage (%)
Received	61	61
Not Received	39	39
Total	100	100

Source: (Survey Data, 2018)

Work Experience of Respondents

The findings were tabulated in the Table II

Table II: Work experience of respondents

Work experience	Frequency	Percentage (%)
Up to 5 Years	16	26
6 – 10 Years	33	54
11 – 15 Years	9	15
16 Years and Above	3	5
Total	61	100

Source: (Survey Data, 2018)

From the findings tabulated in the Table II above, 26% of the respondents had work experience of up to 5 years, 54% had between 6 and 10 years, 15% had between 11 and 15 years while 5% had 16 years and above. This shows that the respondents had the necessary work experience and exposure to provide quality and reliable information to inform our study.

Threats

The various types of security threats experienced or reported in the universities were tabulated using the Likert scale and their respective mean and standard deviation values calculated. The interpretation of the mean values was based on the Likert Scale. The findings were as displayed in the Table III below

Table III: Extent of occurrence of the various types of Security Threats

Security Threats(s)	No Extent 1	Small Extent 2	Moderate Extent 3	Large Extent 4	Very Large Extent 5	Mean	Standard Deviation
	Frequency						
Viruses	0	4	30	13	14	3.61	0.92
Spam	2	16	15	14	14	3.36	1.2
Worms	2	18	21	12	8	3.10	1.02
Hacking attempts	6	23	16	11	5	2.77	1.12
Trojan horse	6	23	21	10	1	2.62	0.93
Adware	13	20	12	11	5	2.59	1.24
Phishing	17	15	16	10	3	2.46	1.21
Denial of Service attacks	15	20	13	13	0	2.39	1.08
Spyware	17	23	10	6	5	2.33	1.22
Spoofing attacks	17	23	16	4	1	2.16	0.97
Brute force attack	19	21	16	5	0	2.11	0.95
Ransomware	21	19	17	2	2	2.10	1.03
Logic Bombs/Time Bombs	18	22	20	1	0	2.07	0.83
Eavesdropping/Sniffing	18	26	16	1	0	2.00	0.8
SQL Injections	19	27	11	4	0	2.00	0.88
Cross-site Scripting	22	21	16	2	0	1.97	0.87
Water hole attack	24	20	15	2	0	1.92	0.88
Man-in-the-middle attacks	24	23	11	3	0	1.89	0.88
Keyloggers	25	20	14	2	0	1.89	0.88
Rootkit	23	26	11	0	1	1.85	0.83
DNS Cache Poisoning	26	22	12	0	1	1.82	0.87

Source: (Survey Data, 2018)

The findings of the research as tabulated in the Table 3 above shows that viruses had the highest mean value of 3.61 and were reported to a moderate extent. Spam with a mean value of 3.36 was second, the third was worms with a mean value of 3.10, followed by hacking attempts with a mean value of 2.77 and trojan horse with a mean value of 2.62.

Adware attacks were reported with a mean value of 2.59 while phishing attacks had a mean value of 2.46. The cyber-attacks least reported in the universities were rootkits and DNS cache poisoning, with mean values of 1.85 and 1.82 respectively. Further, the findings agrees with Ogalo (2012), who found out that virus attacks at 97% were the leading attacks in causing ICT operations disruptions in small and medium enterprises. Further, Raman et al., (2016) established that there was an increase in cybersecurity attacks in institutions of higher learning with the majority emanating from the hacking and malware attacks.

CONCLUSION AND RECOMMENDATION

Firstly, the study contributes to the body of knowledge by specifically answering questions, identifying the threats facing assets in use in the Kenyan public universities. The study findings revealed the security threats experienced in order of prevalence and therefore the universities can institute necessary mitigation controls to curb the security threats and improve on their security posture. In particular, universities need to implement with urgency necessary mitigations to address security threats which were reported to have been experienced to a moderate extent and a small extent namely viruses, spam, worms, hacking attempts, trojan horse, adware, phishing, denial of service, spoofing, brute force, ransomware and SQL injections to avoid risk escalation. Moreover with the onset of coronavirus disease 2019(COVID 19), and evolving nature of security threats it's therefore recommended that universities' management should cause a continual review of the threats to their assets and institute appropriate mitigation controls as per their risk tolerances.

REFERENCES

[1] Abomhara, M., & Koien, G. (2015). Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. Journal of Cyber Security, (4), 65-88.DOI:10.13052/jcsm2245-1439.414

[2] Aineah, A. (2018). Clueless Varsities rewarding hackers with top grades. Standard Digital. Retrieved on March 5th 2019 from https://www.standardmedia.co.ke/article/2001268939/why-research-puts-kenyan-students-fourth-on-list-of-top-hackers-in-africa

[3] Alberts, C. J., & Dorofee, A. J. (2002). Managing Information Security Risks: The OCTAVE Approach. ISBN: 0-321-11886-3

[4] Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (August, 2003). Introduction to the OCTAVE Approach. Carnegie Mellon University

[5] Andreasson, K. (2012). Cybersecurity: Public Sector Threats and Response. ISBN-13:978-1-4398-4664-3

[6] AON. (2019). 2019 Cyber Security Risk Report: What's Now and What's Next. Retrieved from https://cyber.aonunited.com/aon-top-cyber-risks-security-technology-data-digital-transformation?_ga=2.94518748.1915682572.1599053191-1908894240.1599053191

[7] Australian Computer Society. 2016). Cybersecurity: Threats Challenges Opportunities. Retrieved from https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf

[8] BHERT. (2016). Cybersecurity Threats and Responses in the Australian Higher Education Sector. Retrieved from https://www.bhert.com/newsletter/issue-36/cybersecurity-threats-and-responses-in-higher-education-sector

[9] Business Daily. (2017). Slovakian firm cashes in on Kenya Cyber-attacks. Retrieved from https://www.businessdailyafrica.com/corporate/Slovakian-firm-cashes-in-on-Kenya-cyber-attacks/539550-3990046-qs9cihz/index.html

[10] Cloete, N., Bailey, T., Pillay, P., Bunting, I., & Maassen, P. (2011). Universities and Economic Development in Africa. ISBN 978-1-920355-73-9

[11] CPS Research International (2012). Top 100 East African Universities Survey 2012. Retrieved from http://www.cps-research.com/downloads/

[12] Ingerman, B., & Yang, C. (2010). Top-Ten IT Issues, 2010. EDUCAUSE Review, 45(3), Pg 46-60

[13] Joshi, C., & Singh, U. K. (2016). Managing Security Risks and Vulnerabilities in University's IT Threats Landscape. *International Journal of Computer Applications (0975-8887)*. Retrieved from https://pdfs.semanticscholar.org/5382/91c27202872495788c26e7ce30824f58cb51.pdf

[14] Jowi, C. O. N, & Abade, E. (2016). Evaluation of Information Security Risk Assessment for Internet Banking Among Commercial Banks in Kenya. *American Journal of networks and Communications*. 5(3), pp. 51-59. doi: 10.11648/j.ajnc.20160503.11

[15] Njoroge, P. M. (2020). A Framework for Effective Information Security Risk Management in Kenyan Public Universities. Retrieved from http://41.89.196.16:8080/xmlui/handle/123456789/1021

[16] Ogalo, J. O. (2012). The Impact of Information System Security Policies and Controls on Firm Operation Enhancement for Kenyan SMES. *Prime Journal of Business Administration and Management (BAM). ISSN: 2251-1261,* 2(6), 573-581

[17] Pandey, S. K., Mustafa, K. (2012). A Comparative Study of Risk Assessment Methodologies For Information Systems. *Bulletin of Electrical Engineering and Informatics. ISSN: 2089 – 3191,* 1(2), 111-122.

[18] Raman, A., Kabir, F., Hejazi, S., & Aggarwal, K. (2016). Cybersecurity in higher education: the changing threat landscape. *Performance*, 8(3), 46-53. Retrieved from https://consulting.ey.com/cybersecurity-in-higher-education-the-changing-threat-landscape/

[19] Serianu. (2016). Kenya Cyber Security report 2016. Retrieved from http://www.serianu.com /downloads/ KenyaCyberSecurityReport2016.pdf

[20] Shevchenko, N., Chick, T.A., O'Riordan, P., Scanlon, T.P., & Woody, C. (July 2018). Threat Modelling: A summary of Available Methods. Software Engineering Institute|Carnegie Mellon University

[21] Symantec. (2015). Internet Security Threat Report. Retrieved 22nd August 2017, from https://www.symantec.com/content/ en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf

[22] Teng'o, S. (2017, May 11). Cybersecurity: Rise of the Student hacker. Retrieved from https://www.standardmedia.co.ke/ureport/ article/2001239325/cyber-security-rise-of-the-student-hacker

[23] VMware. (2016). University Challenge: Cyber Attacks in Higher Education. Retrieved from https://www.nextgensecurityforeducation.com/wp-content/uploads/VMWare-UK-University-Challenge-Cyber-Security.pdf

[24] Wagstaff, K., & Sottile, C. (2015, September 20). Cyberattack 101: Why Hackers Are Going After Universities. *NBC NEWS.* Retrieved 23rd August 2017, from https://www.nbcnews.com/tech/security/universities-become-targets-hackers-n429821