European Journal of Information Technologies and Computer Science
www.ej-compute.org

Information System Security Practices and Implementation Issues and Challenges in Public Universities

Patrick M. Njoroge, James O. Ogalo, and Cyprian M. Ratemo

ABSTRACT

The use of information and communication technology has been providing the competitive edge for universities globally while Kenyan universities are not an exception. This has in turn made the universities targets of cyber-attacks and hence exposure to unprecedented security risks. The universities need to implement information security best practices and standards in their technological environments to remain secure and operational. The research sought to investigate the information security practices adopted in Kenyan public universities to protect themselves. Descriptive survey method was employed while the study was based on Operationally Critical Threats, Assets and Vulnerability Evaluation (OCTAVE) framework and other industry security best practices. The study targeted the 31 chartered public universities, which were clustered based on their year of establishment. Simple random and purposive sampling methods were utilized to select two target universities per cluster and determine respondents respectively. The study had a response rate of 61%. Analysis of data was done via descriptive statistics while presentation of results was done using tables and Likert scale. The study revealed that universities had implemented information security policies, with 47.6% of respondents somewhat agreeing to that. Funding for security was provided 57.6% somewhat agreeing, though the funding was deemed low by 51% of respondents. Training for security staff was deemed somewhat available (44%) thus below par, while involvement of university management on policies development was at 48% though university management participation in policies review was below average. 38% of respondents somewhat agreed that policies governing use of mobile devices existed. Frequency of user awareness and training was below the average, while 48% of respondents somewhat agreed that universities usually share their intelligence reports on threats and responses with other government agencies. 49% of respondents were somewhat in agreement universities had put in place incidence response plans. Application of updates and improvements was below average, though evaluation of effectiveness of controls was average. To remain protected universities management should cause a review of their employed information security practices and address identified gaps through instigation of essential remedial actions.

Keywords: Assets, information security, information security practices, risks, threats.

Published Online: November 16, 2021

ISSN: 2736-5492

DOI:10.24018/ejcompute.2021.1.5.30

P. M. Njoroge *
Kenya School of Government, Embu, Kenya.
(e-mail: mashnjoro@yahoo.com)
J. O. Ogalo
Kisii University, School of Information Science and Technology, Kenya.
(e-mail: ogalojames@kisiiuniversity.ac.ke)
C. M. Ratemo
Kisii University, School of Information Science and Technology, Kenya.
(e-mail: makiya@kisiiuniversity.ac.ke)

**Corresponding Author*

I. Introduction

Universities operates in an environment having open networks and large amounts of data available for access by the public thus exposing them to several security risks and cyber threats and making them culpable to cyber-attacks [1]. The data comprises of the universities financial data, medical and health information, research data and personal information which is both for the students and the university employees, and students' examinations and grading. Generally, use of technology brings new opportunities and has inherent risks [2], [3]. According to [4] use of information and communication technology has been providing the competitive edge for universities, thus enhancing their capability to execute their fundamental operations and functionalities subsequently increasing their exposure to cyber-attacks.

There is noted growth in security risks every day, due to increased frequency of attacks, which have become easy, automated, and sophisticated [4]-[6]. Globally 10 % of all the internet security threats recorded were directed at the education sector [7]. 36% of universities in the United Kingdom were reported to be experiencing cyber-attacks on

an hourly basis [8]. Between the year 2006 and 2013, in the United States, 550 universities had reported some form of data breaches [5]. Several universities were recorded to have had cyber-attacks, which compromised their servers and their database records, disrupted network functionality, and caused data breaches and website hacking [1]. A survey by CPS International in 2012 showed that universities in Kenya were way ahead in use of ICT, compared to others in the East African region [9].

A cyber security report for Kenya [10], uncovered the leakage of Ministry of Foreign Affairs data, hacking of twitter handle for University of Nairobi and web defacements. The rise of cyber-attacks directed at Kenyan universities with an aim of tampering with grades of students, fee balances, records of students and employees was recorded [11]. If universities ICT systems and their critical data is not properly protected negative aftermaths could result including disruption of provision of critical services, loss of revenue, reputation damage, disruption to network functionality and damage or loss of valuable data. Universities need to implement information security practices based on industry best practices and internationally recognized standards to guarantee confidentiality, availability and integrity of their critical data, and information systems, and hence defend themselves against cyber-attacks [12].

II. Statement of the Problem

The use of information and communication technology has been providing the competitive edge for universities globally particularly in execution of their core operations and functionalities, and Kenyan universities are not an exception. This has in turn continually made the universities targets of cyber-attacks and hence exposure to unprecedented security risks. The growth of security risks undermines the availability, integrity, and confidentiality of the universities sensitive data and ICT systems, thus prompting for positive responses and institution of information security best practices and standards in their technological environments to remain protected and operational. The study examined the information security practices implemented by universities against the industry best security practices and standards, with an aim of identifying gaps and apprise on necessary actions to institute.

III. Objective of the Study

The primary objective was to analyze Information security practices and implementation in public universities.

IV. Literature Review

A. Assets

An asset refers to the software, data, hardware, business activities and processes, information, and network infrastructure. Assets are very critical in fulfilment of the mission and objectives of a business [13]. It's imperative that universities assets used in their core operations and functionalities be protected from incidents, security breaches, vulnerabilities and threats which can impact negatively on the universities if lost, destroyed, modified, or accessed without authorization.

B. Catalog of Information Security Practices

Information security practices refers to actions currently been utilized by the organization to initiate, implement, and maintain its internal security. The information security practices do offer protection to the organization's assets and other information-related assets [13]. The information security practices currently employed by the universities need to be established and then compared against best practices in the industry security standards [14]. By doing this, universities are able to comprehend how well they could be fairing security wise, and any gaps identified can be addressed by instituting crucial remedial actions [13], [15]. The researcher did investigate several information security practices anchored on OCTAVE and other industry best practices to determine the extent to which the universities had initiated and implemented the information security practices and thereby identify weaknesses or gaps. The investigated information security practices included availability of security policies in the universities, training for the security function , provision of funding or sufficient budget for the security function, users and management security awareness, availability and implementation of policy on use of mobile devices, review of security policies ,involvement of management in the development and the implementation of the security policies, incidence response plans, updates and improvements, sharing of intelligence of threats and responses with other government agencies and lastly evaluation of effectiveness of instituted controls.

C. Theoretical Framework

The study was anchored on Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) framework for assessing the information security practices and other industry security best practices. OCTAVE criteria, R01.4 is a key output which involves identifying the executed information security practices, which guarantees protection of universities assets and other information-related assets [15]. OCTAVE contributes directly to risk management, its flexible and its well-documented, and actually leverages on the knowledge of the people working within an organization hence it strategically addresses information security risks requirements of public universities in Kenya as compared to other industry standards such as ISO 27001, NIST Framework, ISO 27005 and CCTA (Central Communication and Telecommunication Agency) Risk Analysis and Management Method (CRAMM) [16].

V. Methodology

The research was undertaken in Kenyan public universities. Descriptive survey method was employed while both quantitative and qualitative data was collected to assist in answering the research questions. The 31 chartered public universities were clustered into two according to the actual year when they were made fully-fledged universities [15].

A sample of four universities was selected, two from every cluster using simple random technique. Purposive sampling was utilized to determine the respondents for the survey that

is personnel from the computer science and information and communication technology departments. Respondents therefore were Systems Administrators, Security Administrators, ICT Officers, Web Administrators, IT Support, IT Managers, IT Technologists, Database Administrators, Network Administrators, Systems Analysts, and IT Technicians [15], [16]. The target population was a hundred respondents. The data collection tool utilized was a questionnaire while data analysis was done using descriptive statistics and results presentation done via Likert scale and tables. The questionnaire used for data collection was subjected to expert review to ensure that it measured what was intended and a pre-test study was carried out.

VI. Results and Discussion

The findings of the research and subsequent discussion are presented.

A. Catalog of Information Security Practices

1) Information Security Policy

Availability of an information security policy in an organization is a fundamental statement to the stakeholders as well as the outside world that the organization is committed to security. A good information security policy serves to protect information and systems of an organization as well as the employees and the whole organization. Results as per Table I indicate that majority of the respondents (56%) somewhat agreed that universities had information security policies in place, while a further 18%
strongly agreed. This was noted to be in agreement with the findings of [17], that majority of enterprises have information security policies in place.

2) Training to Build Capacity for Security Function

The respondents (44%) did somewhat agree and a further 5% strongly agreed that universities do train their staff who handle the security functions. This was noted to be below average while ISO 27001:2013 standard requires that staff training be prioritized to make sure that the staff handling the security functions have the right skills and competences. Therefore, the universities management should prioritize capacity building for their security staff.

3) Management Provides Necessary Funding for the Security Functions

The respondents (57.6%) somewhat agreed and a further 9.8% were strongly agreeing that the university management supports security functions by providing funding required. However, as per Table II, majority of the respondents (51%) were of the opinion that the security funding/budget which was provided was actually low. Moreover, 15% of the respondents believed no budget existed for the security function in their universities. Inadequate security funding is a danger to the effective deployment of an information management system [18]. To guarantee that their critical information systems were protected 85% of universities in the United Kingdom were seeking more funding/budget for their security functions [8]. Since provision of funding/budget for the security function was established to be low in Kenyan public universities, universities management should provide sufficient funding/budget for the security functions to guarantee continued protection.

TABLE I: Security Funding /Budget

Security Funding/Budget	Frequency	Percentage (%)
High	2	3
Moderate	19	31
Low	31	51
No Budget Exists	9	15
Total	61	100

TABLE II: CATALOG OF INFORMATION SECURITY PRACTICES SOURCE (SURVEY DATA, 2018)

Catalog of Security Practices	Strongly Agree		Somewhat Agree		Don't Know/ Unfamiliar		Somewhat Disagree		Strongly Disagree	
	Freq.	(%)	Freq.	(%)	Freq.	(%)	Freq.	(%)	Freq.	(%)
University has security policies in place	11	18	34	56	4	6.5	6	9.8	6	9.8
Training to build capacity for security function	3	5	27	44	4	6.5	14	23	13	21.5
Management provides necessary funding for the security functions	6	9.8	35	57.6	3	5	9	14.6	8	13
Awareness for users and management carried out periodically	3	5	23	37.4	3	5	15	24.7	17	27.9
Users' awareness of their security roles and responsibilities	4	6.5	28	46	2	3.3	14	23	13	21
University has incidence response plans in place	3	5	30	49	5	8.1	8	13	15	24.9
Mobile devices policies in place	8	13	23	37.7	8	13	12	19.6	10	16.7
Management involvement in development and implementation of security policies	6	9.8	29	47.6	4	6.5	12	19.9	10	16.2
Management involvement in review of security policies	5	8.1	22	36	3	5	16	26.2	15	24.7
Management awareness of their security roles and responsibilities	2	3.3	29	47.6	3	5	17	27.9	10	16.2
Necessary updates and improvements on the security policies and other plans	5	8.1	22	36	3	5	16	26.2	15	24.7
Sharing of intelligence with other government agencies on threats and responses	8	13	29	48	7	11.5	6	9.8	11	18
Evaluation of the effectiveness of controls	5	8.1	27	44	5	8.1	12	20	12	19.9

4) User's Awareness of Their Security Roles and Responsibilities

The study revealed that 46% of the respondents, somewhat agreed while a further 6.5% strongly agreed that in terms of security the users of the university systems understood their responsibilities. However, the combined percentage of 52.5% was slightly above average, implying that more efforts should be directed towards user awareness to guarantee security in the universities.

5) Management Awareness of Their Security Roles and Responsibilities

47.6% of the respondents did somewhat agree that the university management understood their roles and responsibilities in matters of security while a further 3.3% of the respondents did strongly agree. The rating was just average with a combined percentage of 50.9%.

6) Frequency of Users and Management Awareness and Training

The respondents (37.4%) somewhat agreed while another 5% strongly agreed that awareness and training is done periodically. The combined percentage of 42.4% was below the average mark of 50%. User awareness and training was noted to be effective at responding and preventing security breach incidents [19], even though many organizations lacked it. Lack of user training and awareness was identified as a possible impediment to effective deployment of information security management systems [18]. Universities management should direct more efforts towards training and awareness and increase the frequency of the same.

7) University Has Incidence Response Plans in Place

The study revealed that the respondents (49%) somewhat agreed while a further 5% strongly agreed that universities were having incidence response plans. The rating was slightly above average with a combined percentage of 54%. An incident is basically an attack against any information asset which is a clear threat to the confidentiality, integrity, or availability of information resources. An incident response plan therefore includes the identification of, classification of, and response to an incident [20]. Universities preparedness to respond to clear attacks which are a threat to the confidentiality, integrity, or availability of their systems and information resources is critical.

8) Mobile Devices Policies in Place

The respondents (37.7%) somewhat agreed while 13% strongly agreed that mobile policies had been implemented in universities to govern the use of mobile devices in their computing environments. The rating was just average with a combined percentage of 50.7%. Security concerning mobile devices was noted to be inadequate for most of the organizations, thus exposure to security risks [19]. Mobile devices are seen as easy entry point of attacks into a network, presenting security risks [21] thus universities should implement mobile policies to govern access and use of resources by these devices in their network and computing environments.

9) Management Involvement in Development and Implementation of Security Policies

The study revealed that 47.6% of the respondents somewhat agreed and another 9.8% strongly agreed that management is actively involved in development and employment of security policies. ISO 27001:2013, requires that top management be involved in development and employment of information security policies in their organizations, as a best practice.

10) Management Involvement in Review of Security Policies

The respondents (36%) somewhat agreed that the university management is involved in the review of the information security policies which was deemed to be below the average mark of 50%. As a best practice universities management should be actively involved in the review of information security policies.

11) Sharing of Intelligence with Other Government Agencies on Threats and Responses

48% of the respondents somewhat agreed while another 13% strongly agreed that universities do share their intelligence on threats and the responses with other government agencies. This was a positive gesture towards learning from other agencies.

12) Necessary updates and Improvements on the Security Policies and Other Plans

The respondents (24.7%) strongly disagreed while another 26.2% somewhat disagreed with the statement that updates and necessary improvements on the security systems and other plans are executed. A security information management system which does not incorporate updates and improvements is at risk of being obsolete and becoming insecure.

13) Evaluation of the Effectiveness of Controls

The respondents (44%) somewhat agreed while another 8.1% strongly agreed that controls which are implemented are actually evaluated for effectiveness.

VII. Conclusion and Recommendation

The study revealed that the initiation, implementation, and maintenance of the information security practices in the universities was imperfect. Since the information security practices are used to protect the universities' assets and information-related assets, it's critical for universities management to cause a review of their implemented information security practices. Identified gaps or any missing interventions should be remedied to guarantee protection. Similar studies can be carried out for private universities and other institutions within the education sector in Kenya. Deficiencies were identified in areas pertaining funding, training, user awareness, review of information security policies, implementation of policies to govern mobile devices, and updates and improvements which was below average. Moreover, in view of the onset of coronavirus disease 2019 (COVID-19), and evolving nature of security threats and technological adoption, in universities it's recommended that universities' management should cause a continual review of their implemented information security practices to keep abreast.

REFERENCES

[1] Raman A, Kabir F, Hejazi S, Aggarwal K. Cybersecurity in higher education: the changing threat landscape. *Performance.* 2016; 8(3): 46-53.
[2] Andreasson KJ. *Cybersecurity: public sector threats and responses*. Taylor & Francis, 2011.
[3] Australian Computer Society. Cybersecurity: Threats Challenges Opportunities. 2016.
[4] BHERT. Cybersecurity Threats and Responses in the Australian Higher Education Sector. 2016. Available from https://www.bhert.com/newsletter/issue-36/cybersecurity-threats-and-responses-in-higher-education-sector.
[5] Wagstaff K, Sottile C. (2015). Cyberattack 101: Why hackers are going after universities. *NBC News*.
[6] Pandey SK, Mustafa K. A comparative study of risk assessment methodologies for information systems. *Bulletin of Electrical Engineering and Informatics.* 2012; 1(2): 111-122.
[7] Symantec. Internet Security Threat Report. [Internet] 2015. [cited on August 22 2017] Available from: https://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf.
[8] VMware. University Challenge: Cyber Attacks in Higher Education. [Internet] 2016. Available from: https://www.nextgensecurityforeducation.com/wp-content/uploads/VMWare-UK-University-Challenge-Cyber-Security.pdf.
[9] CPS Research International (2012). *Top 100 East African Universities Survey 2012.* Available from http://www.cps-research.com/downloads/
[10] Serianu. (2016). *Kenya Cyber Security report 2016.* Available from http://www.serianu.com/downloads/KenyaCyberSecurityReport2016.pdf.
[11] Teng'o, S. *Cybersecurity: Rise of the Student hacker.* [Internet] 2017. Available from: https://www.standardmedia.co.ke/ureport/article/2001239325/cyber-security-rise-of-the-student-hacker.
[12] Wilshusen GC, Powner DA. *Cybersecurity: Continued Efforts Are Needed to Protect Information Systems from Evolving Threats.* Government Accountability Office Washington DC. 2009.
[13] Dorofee CAA. Managing information security risks: the OCTAVE (SM) approach. 2002.
[14] Alberts C, Dorofee A, Stevens J, Woody C. *Introduction to the OCTAVE Approach.* Carnegie Mellon University. 2003.
[15] Njoroge PM. An Examination of Threats facing Assets in Use in Kenyan Public Universities. 2021.
[16] Njoroge PM. (2020). A Framework for Effective Information Security Risk Management in Kenyan Public Universities. 2020.
[17] Ogalo JO. The Impact of Information System Security Policies and Controls on Firm Operation Enhancement for Kenyan SMES. *Prime Journal of Business Administration and Management (BAM).* 2012; 2(6): 573-581.
[18] Wechuli NA, Muketha GM, Matoke N. Cyber Security Assessment Framework: Case of Government Ministries in Kenya. *International Journal of Technology in Computer Science and Engineering.* 2014; 1: 2349-1582.
[19] IBM Security. Security Threats, Frameworks and Mitigation Efforts: How Can You Lower Your Risk. 2016. Available from: https://www.rsaconference.com/writable/presentations/file_upload/sop-05_security_threats_frameworks_and_mitigation_efforts_how_can_you_lower_your_risk_final2.pdf.
[20] Whitman ME, Mattord HJ. *Principles of Information Security.* Cengage Learning. 2012.
[21] WaterISAC. 10 Basic Cybersecurity Measures: Best Practices to Reduce Exploitable Weaknesses and Attacks. 2016. Available from: https://ics-cert.us-cert.gov /sites/default/files/documents/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_S508C.pdf.