The Journal of Informatics, Vol. 1, Issue 1 (pages 1-12)
ISSN 2714-1993
Received: September, 2020, Published: March, 2021

_____***Original Research***_____

CYBERSECURITY POSTURE OF HIGHER LEARNING INSTITUTIONS IN TANZANIA

Authors
Baraka Mtakati
Department of ICT
Arusha Technical College, Arusha, Tanzania

&

Frank Sengati
Department of Informatics
Institute of Accountancy Arusha

Abstract
In a bid to become a middle-income country by 2025, the Government of the United Republic of Tanzania promoted the productive use of ICT for rapid development, which is why Higher Learning Institutions (HLIs) adopted information systems to handle admission matters. Urgent response to directives without enforcing credible cybersecurity measures is a massive security vulnerability that cyber attackers can exploit. This study assessed the cybersecurity preparedness of HLIs in protection, detection, and response to cyber-attacks using the NIST cybersecurity framework. To achieve this objective, a qualitative method and an interpretive research approach were adopted. The target population was four (4) Higher Learning Institutions located in Arusha Municipality. A purposive sampling technique was used due to an inadequate number of cybersecurity experts in the population. Empirical data were collected using semi-structured, face-to-face interviews, documentary reviews, observation, penetration testing and analyzed using content analysis. Despite implementing minimal countermeasures, the study discovered that Higher Learning Institutions are vulnerable to cyber-attacks. Higher Learning Institutions must be vigilant by; addressing identified weaknesses, providing cybersecurity training to all staff, and continuously monitoring information systems. The study recommends a need to explore the factors affecting cybersecurity preparedness in Higher Learning Institutions.

Keywords – Cybersecurity Posture, Cybersecurity Preparedness, Higher Learning Institutions, Cybersecurity Framework

1.0 INTRODUCTION

The government of the United Republic of Tanzania recognizes the effective use of Information and Communications Technology (ICT) as a critical factor for rapid socio-economic growth (Ministry of Works, Transport and Communication, 2016). Higher Learning Institutions, as key players for socio-economic growth, are obliged to provide reliable services, sustain good citizen-to-government communications, and protect confidential information (CISCO Report, 2015). According to Tanzania Commission for Universities, students' enrollment in Higher Learning Institutions in Tanzania increased tremendously from 44,715 students in 2012/13 to 63,737 students in 2017/18 (Tanzania Commission for Universities, 2018). To improve the quality of admission and registration services offered by Higher Learning Institutions, Tanzania Commission for Universities issued a directive on data sharing via API (Tanzania Commission for Universities, 2018). Urgent response to ICT directives without developing and implementing reliable cybersecurity countermeasures is a massive security flaw. Cyber-attackers can utilize this security flaw to distress the confidentiality, integrity, and availability of implemented information systems (Zwilling et al., 2019).

Despite improving the quality of services offered by Higher Learning Institutions, the advancement of ICT has also created a conducive environment for cyber-attackers to exploit existing vulnerabilities (Naden, 2019). An exponential increase in sharing data across the internet and between devices exposes HLIs to an ever-widening range of cybersecurity risks (International Telecommunication Union, 2018). An average of 19,800 records was compromised in each Australian data breach in 2018 (Edith Cowan University, 2019). Serianu (2018) depicted an increase in an estimated loss of US$1.5bn to African businesses because of cyber-attacks. Nigeria was greatly affected by losses of US$649m, followed by Kenya with US$210m and Tanzania with US$99m. In 2017, the

website of the Open University of Tanzania was hacked (Matandiko, 2017). Information systems audit conducted by Controller and Auditor General in HLIs of Tanzania from 2017 to 2019 revealed massive cybersecurity vulnerabilities that could be exploited by cyber-attackers (National Audit Office of Tanzania, 2020). To address the risks posed by cyber-attackers, institutions must be vigilant by having a required level of cybersecurity preparedness in identifying, protecting, detecting, responding, and timely recovery to normal operations to reduce the impact of cybersecurity incidents (NIST, 2018). Cybersecurity preparedness is mandatory for the optimal performance of Higher Learning Institutions (Zegers, 2016). It is crucial for HLIs to safeguard their information systems and data in cyberspace to guarantee the provision of uninterrupted ICT services to their clients (Kumar, 2017).

Cyber threats are growing exponentially in Tanzania Institutions (Lubua and Pretorius, 2019; Adams, 2017). Tanzania Computer Emergency Response Team reported a dramatic 54% increase in network attacks in Tanzania from 314,909 attacks in January 2019 to 583,147 attacks in January 2020 (Tanzania Computer Emergency Response Team, 2020). Despite several studies conducted globally in the area of cybersecurity (Baino, 2016; Sithole, 2019; Makumbi et al., 2018 and Nyamongo, 2015), they did not address the cybersecurity preparedness of Higher Learning Institutions in Tanzania. Tanzania Commission for Universities, as a regulatory body with a mandate to recognize, approve, register, and accredit universities in Tanzania, has not yet conducted a study on the cybersecurity preparedness of its Institutions. Tanzania Communications Regulatory Authority, as a quasi-independent government body responsible for regulating the communications and broadcasting sectors in Tanzania, has also not yet conducted a study on the cybersecurity preparedness of HLIs (Tanzania Communications Regulatory Authority, 2020).

2.0 OBJECTIVE OF THE STUDY

This study assessed the cybersecurity preparedness of HLIs using the NIST cybersecurity framework (NIST CSF). NIST CSF was selected because it is considered as a high-level abstraction of related frameworks. It provides references to other related frameworks for specific implementation guidelines. Referenced frameworks include: NIST SP 800-53 Rev. 4, COBIT5, ISO/IEC 27001:2013, ISA 62443-2-1:2009, ISA 62443-3-3:2013 (Ibrahim et al., 2018).

3.0 LITERATURE REVIEW

Baino (2016) from Australia conducted a safety risk assessment survey related to networked information systems. The research results showed that a large proportion of safety lapses result from system administrators not updating software patches and failing to keep up with innovations in their business. He recognized the system administrator's ineffectiveness to culture and workload, saying that in most instances, system

administrators are accountable for taking care of countless disparate structures. He also discovered that system administrators are also expected to be specialists in increasingly complex systems consisting of different techniques beyond the understanding of most of them. However, the study did not recognize detection and response activities as crucial components toward cybersecurity preparedness.

In Sweden, Kreicberga (2017) conducted a study on inner risk in tiny and medium-sized businesses (SMEs) to data safety countermeasures and the human factor. Results of the studies were that official policies that lack adequate maintenance and consciousness do not affect staff conduct, while informal standards within the organization have the most significant influence on conduct in information security. Countermeasures to technological safety are more efficient and taken seriously if their necessity is described as an advantage to end customers. The study fell short of recognizing a lack of training, access control, vulnerability scans, and response plans as critical safety countermeasures.

Sithole (2019) surveyed South African public sector organizations to assess the cybersecurity preparedness of the information systems, that is, the capability to anticipate, withstand, detect, respond to, recover from, and adapt to any disastrous cyber incidents with an ability to resume services at an acceptable level and time. Findings from this study revealed that the South African public sector organizations are more vulnerable to cyber risks due to a lack of essential cybersecurity control requirements, namely: a cyber-security strategy, an adequate skilled workforce, an effective incident response plan, a cyber-risk management strategy, a cyber-security awareness program as well as clearly defined cybersecurity roles and responsibilities for the executive management and senior management. However, the study did not address the effectiveness of protection and detection measures through penetration testing (Engebretson, 2011).

Makumbi et al. (2018) conducted a study in Kenyan small and medium-sized companies (SMEs). The study aimed to determine the amount of reliance Kenyan SMEs have on ICT, identify the most common safety threats among Kenyan SMEs, and determine how Kenyan SMEs protect their pcs, data, and networks against information security hazards. The research results were that the organizations investigated were aware of the significance of the safety of information systems and tried to put in place safety measures based on their dependence. Based on the nature of these organizations under study, economic fraud appeared to feature prominently among the reported events, computer asset loss seemed to be a recurring issue, and system user danger was prevalent among the studied organizations. The prevalent defence used against hacking is firewalls. The study suggested that such organizations put numerous steps in place, including task segregation, physical security controls, and IT asset inventories. He also

suggested user awareness campaigns to raise awareness about ICT safety (Makumbi, 2018). The study relied on protection measures only, and there is a need to assess the detection of cyber-attacks and the ability to respond to detected cyber incidents.

Nyamongo (2015) surveyed the safety leadership of data systems, a case study of chartered private colleges in Kenya. Research results shown that Higher Learning Institutions in Kenya are willing to embrace and enhance the safety management of their data systems by frequently updating the management on safety updates. Training of staff in information systems security management will improve the management of the university's information security system a great deal (Nyamongo, 2015). The significant difficulties facing information system management were viruses, user mistakes, computer robbery, system and software bugs. The research found that Higher Learning Institutions should rethink their methods of managing the safety of their most valued resources, including adopting efficient management of information security (Nyamongo, 2015). The study fell short of assessing the ability of Higher Learning Institutions to respond to cyber incidents (NIST, 2018)

Kundy and Lyimo (2019) assessed the cybersecurity threats in Higher Learning Institutions in Tanzania, a case of the University of Arusha and Tumaini University Makumira. The purpose of the study was to investigate the cybersecurity threats faced by Higher Learning Institutions, to evaluate the cyber threat countermeasures that the University of Arusha and Tumaini University Makumira have put in place, and lastly, the study proposed the proper cybersecurity threat framework for the University of Arusha and Tumaini University Makumira. Findings from the study revealed that cyber threats are influenced by; negligence of management in implementing cybersecurity strategies, weak ICT infrastructures, and poor cybersecurity awareness of employees. The study did not assess the ability of Higher Learning Institutions to detect and respond to cyber incidents.

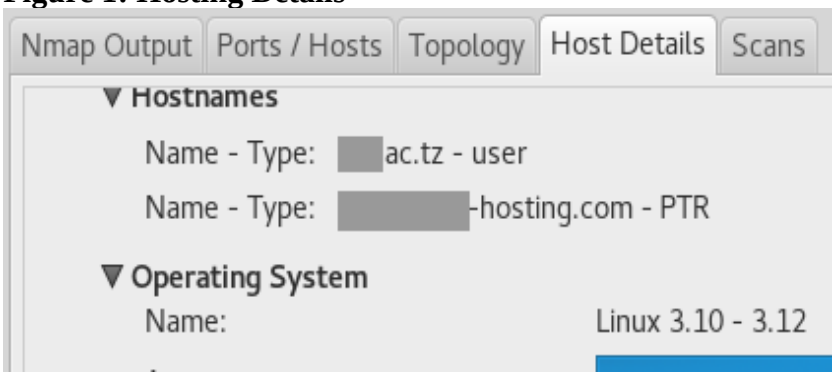
Based on the above empirical literature review, it is evident that extensive research has been done in developed and neighbouring countries such as South Africa and Kenya. The case studies reviewed revealed that organizations are aware of cybersecurity risks and minimal protection measures were in place (Baino 2016; Makumbi et al. 2018; Kundy and Lyimo, 2019). However, the effectiveness of the implemented protection measures was not assessed using an internationally recognized framework. Detection and response mechanisms were not recognized as critical factors towards cybersecurity preparedness. In other studies, Sithole (2019) and Kreicberga (2017) conducted their research on cybersecurity preparedness in non-higher learning institutions. These studies are irrelevant in the context of cybersecurity preparedness of Higher Learning Institutions in Tanzania. Generally, there is no adequate information about the cybersecurity preparedness of Higher Learning Institutions in Tanzania. This study filled

the gap by; assessing the effectiveness of cybersecurity protection measures, examining cybersecurity detection mechanisms, and evaluating cybersecurity response mechanisms of higher learning institutions in Arusha Municipality using NIST Framework.

4.0 METHODOLOGY

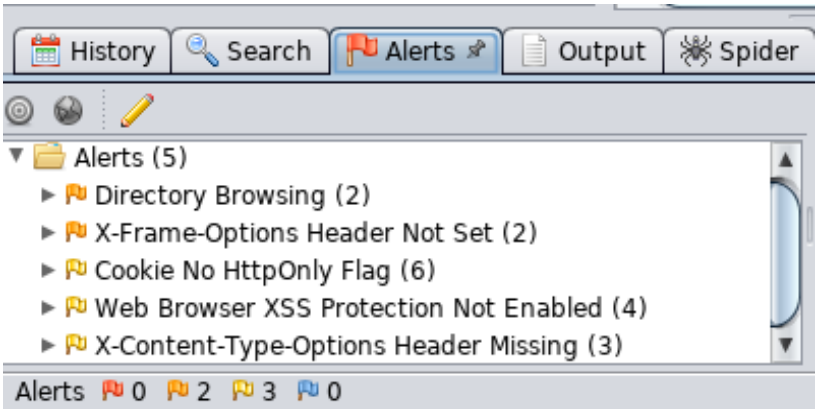
A qualitative method and an interpretive research approach were adopted to provide a starting point in understanding the cybersecurity mechanisms used by HLIs from experienced cybersecurity experts (Myers, 2013). The target population was all four (4) Higher Learning Institutions located in Arusha Municipality; Arusha Technical College (ATC), Eastern and Southern African Management Institute (ESAMI), Institute of Accountancy Arusha (IAA), and St. Augustine University in Tanzania-Arusha Centre (SAUT). The reasons for choosing this study area are; it has a combination of private and government-owned institutions, it was very familiar to the researcher, it was inexpensive and easy for the researcher to get the information needed in data collection. The purposive sampling technique was used due to the limited number of people with knowledge and experience of cybersecurity in the study population. Data were collected using semi-structured face-to-face interview, documentary review, observation, and penetration testing. The black-box model approach with reconnaissance, scanning and exploitation phases were used during Penetration Testing (Engebretson, 2011). The researcher used several tools of Kali-Linux during Penetration Testing: Zenmap tool was used for reconnaissance (Figure 3.1), Owasp ZAP was used for scanning (Figure 3.2), Sqlmap was used for exploiting SQL injection vulnerability in web-based admission systems (Figure 3.3)

Figure 1: Hosting Details



Source: Research Field Data (2021)

Figure 2: Scanning Web-based Admission System



Source: Research Field Data (2021)

Figure 3: Exploiting SQL Injection Vulnerability

Source: Research Field Data (2021)

Content analysis was used to analyze the collected data referring to the NIST cybersecurity framework. This framework provides a reference model of continuous cyber risk management that creates an effective cybersecurity program and improves the resilience of information systems and critical infrastructures. The NIST Cybersecurity Framework has five core functions: identity, protect, detect, respond, and recover (NIST, 2018). Protect, detect, and respond are considered the most critical core functions (Blum, 2020; CISCO Report, 2015; Naden, 2019). Categories and sub-categories with these three core functions were used in this study. To ensure validity and reliability in this study, triangulation and thick descriptions were used (Brink,1993).

Figure 4: Core Functions of the NIST Framework

Source: NIST (2018)

5.0 RESULTS AND DISCUSSION

This section analyzes, interprets, and discusses data from the field. The findings focused on the "assessment of cybersecurity preparedness using the NIST framework: a survey of higher learning institutions in Arusha municipality". The study assessed the cybersecurity protection measures adopted by Higher Learning Institutions, determined the cybersecurity detection mechanisms implemented, and evaluated the response mechanisms employed by Higher Learning Institutions.

4.1 Protection Against Cyber Attacks

The study discovered that all 4 (100%) Higher Learning Institutions had protected network integrity using VLAN, physical and remote access controls such as CCTV cameras, physical checkpoints in entry gates, access logbooks in server rooms, and VPN are in place. However, there is uncertainty about whether security controls for both remote access and physical access are regularly maintained, monitored, and reviewed. Higher Learning Institutions must be proactive in reviewing, monitoring, and maintaining security controls to improve them and fix any loophole that attackers might use. While it is essential to regularly test information systems to ensure that they can detect, withstand, respond to, and recover from cyber-attacks (NIST,2018), the findings revealed that all 4 (100%) Higher Learning Institutions surveyed have never tested their existing information systems for cybersecurity preparedness. In protective technology, 1 out of 4 (25%) institutions have protected and restricted removable media usage. 75% of the institutions surveyed nodo not have protection and restrictions against removable media. Improper handling of removable media exposes institutions to the risk of being attacked and used as distribution points of malicious files over the internet. In the case of cyber-workforce, the study found insufficient resources to deal with cybersecurity matters in all 4 (100%) institutions, and none had a cybersecurity department with skilled and trained staff responsible for cybersecurity. This makes surveyed Higher Learning Institutions more vulnerable as they lack the skilled staff to manage and

contain cybersecurity-related risks. In data security, the findings revealed that all institutions were doing the backup, protection against data leaks was implemented. However, even though data protection is partially covered in other security documentation such as ICT policy, Higher Learning Institutions do not have a Data Loss Prevention Strategy to counter data breaches. This finding contrasts with the data security category of NIST (2018). Institutions must have a Data Loss Prevention Strategy to manage data breach incidents accordingly. In information protection processes and procedures, backups are conducted and maintained. However, the study revealed that backups are not tested. Higher Learning Institutions must test their backup files to ensure that they have an uncorrupted backup copy of the original data, and that data can be retrieved whenever needed.

4.2 Detection of Cyber Incidents

The study found that out of 4 institutions, only 1 (25%) was monitoring unauthorized connections and devices. In the other 3 (75%) institutions, a stranger can use plug and play devices to connect to an internal network and access vital services. Effective and efficient network monitoring and detection necessitate the use of integrated technologies (Tenable Network Security, 2013). All four institutions (100%) were found to use an intrusion detection system such as fail2ban in the monitoring network to detect potential cybersecurity events, updated antiviruses were used to detect malicious code, and detection processes were continuously improved, this is in line with the literature as Anderson (2017) argued that effective ways to analyze and prevent cyber incidents are to conduct continuous monitoring and searches for threats. The study found that institutions have not established the baseline of network operations and data flows, contrary to O'Neill (2016), who emphasized that documenting baseline readings for network traffic is the foremost course of action to identify potentially suspicious activities efficiently. Kerravala (2016) and AT&T Cybersecurity (2018) agreed on the criticality of establishing a network baseline for what amounts to the normal performance of the network. Furthermore, the study revealed that the physical environment and personnel activities are not monitored to detect potential cybersecurity events. This weakness must be addressed to deny unauthorized access to sensitive areas of the institution and handling suspicious personal activities before they become harmful.

4.3 Response to Cyber Attacks

The study found that all four (4) visited institutions (100%) did not have a cybersecurity response plan, which implies that they cannot execute and sustain response processes and procedures to ensure timely response to detected cybersecurity incidents. Due to a

lack of response plan, there is a lack of sufficient coordination to allow organized response activities with internal and external stakeholders, which in turn reduces the capacity of Higher Learning Institutions to contain and mitigate cybersecurity incidents (NIST, 2018). Furthermore, the study found that forensic investigations are not performed due to a lack of tools and experienced professionals. Due to this, institutions are unable to determine the cause of cyber-attacks, collect any valuable evidence, and examine any digital data found on the crime scene (Lillis et al., 2016). This deprived institutions the opportunity to learn from cyber-attacks and improve their cybersecurity controls to ensure effective protection, detection, and timely response to future cyber-attacks. The following must be carried out to provide adequate response mechanisms: to establish an incident response plan for cyber incidents; to establish a data breach notification protocol to interact and coordinate response activities with internal and external stakeholders; perform analysis to ensure effective response; prevent the expansion of cyber-attack, mitigate its effects and resolve the incident; improve response activities by learning from the current and previous response activities.

6.0 CONCLUSION

The objective of this research study was to assess the cybersecurity preparedness of Higher Learning Institutions since there is no complete defence against ever-increasing and sophisticated cyber threats and cyber-attacks. This research found that the Higher Learning Institutions surveyed are more vulnerable to cyber-attacks due to a lack of appropriate cybersecurity measures such as; assessment of the cybersecurity posture of third-party service providers, cybersecurity strategies, under-reporting or non-reporting of all their experience of cyber incidents. There is also no reliable information that can make other organizations aware of the need to strengthen their security methods and solutions. This is demonstrated by a lack of cooperation within HLIs and with other industries.

For Higher Learning Institutions to be prepared, they need to address basic cybersecurity requirements, such as the development and implementation of cybersecurity policy and an incident response plan, to invest in an adequate skilled cyber workforce and cybersecurity education, training, and awareness programs, to invest in advanced technical security solutions, and to encourage and enforce cyber risk management. These controls will provide a green light towards achieving cybersecurity preparedness. Cybersecurity preparedness must therefore be seen as a crucial strategic priority in the evolution of digital institutions, as it is a key factor in the rapid and efficient recovery and continuous operation of information systems. It is important that Higher Learning Institutions not only ensure the security of important resources and information systems

but that service delivery continues to occur even in the event of a cyber-incident. This study was restricted mainly to Higher Learning Institutions located in Arusha municipality. Therefore, it may not be suitable to generalize its findings in this nation or any other nation to the entire population of institutions. Further empirical studies are therefore required in distinct areas as well as in other East African nations.

REFERENCES

Adams, Y. (2017) *Computer Security Technology Planning Study*. Retrieved 21 08, 2020, from National Institute of Standards and Technology, Information Technology Laboratory: http://csrc.nist.gov/publications/history/ande72.pdf

AT&T Cybersecurity (2020) *Establishing Baseline Network Behavior*. [Online] Available at https://cybersecurity.att.com/documentation/usm-appliance/getting-started/baseline-behavior.htm [Accessed 10 May 2020]

Anderson, E. (2017) *Blog: How to Comply with the 5 Functions of the NIST Cybersecurity Framework*. [Online] Available at: https://www.secmatters.com/blog/how-to-comply-with-the-5-functions-of-the-nist-cybersecurity-framework [Accessed 15 May 2020].

Australian Securities and Investments Commission (2015) *Cyber resilience: Health check*. [Online] Available at: https://download.asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf [Accessed 15 June 2020].

Baino, T. (2016) *Evaluation of Security Risks Associated with Networked Information Systems*. Melbourne: Royal Melbourne Institute of Technology University.

Blum D. (2020) *Institute Resilience Through Detection, Response, and Recovery. In: Rational Cybersecurity for Business.* Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-5952-8_9

Brink H. I. L. (1993) *Validity and Reliability in qualitative research*. Paper delivered at SA Society of Nurse Researchers" Workshop-RAU, UNISA: Department of Nursing Science Vol 16, No 2. Retrieved March, 16th 2020, from https://www.curationis.org.za/index.php/curationis/ article/ download/1396/1350.

CISCO Report (2015) *what-is-cybersecurity.aspx*. Retrieved from http://www.itgovernance.co.uk:http://www.itgovernance.co.uk/whatiscybersecurity.aspx

Edith Cowan University (2019) *ECU | Cyber-attacks cause data breach costs to soar: News: News*. Available at: https://www.ecu.edu.au/news/latest-news/2019/08/cyber-attacks-cause-data-breach-costs-to-soar (Accessed: 7 March 2020).

Engebretson, A. (2011) *The Basics of Hacking and Penetration Testing*. Waltham, Elsevier Inc

Heidi W.M. (2017) *Countering Social Engineering through Social Media*: An Enterprise Security Perspective. Australia: Charles Sturt University.

International Telecommunication Union (2016) *New Security Threats Invade Africa in 2016*. Retrieved 21 08, 2020, from IT News Africa: http://www.itnewsafrica.com/

International Telecommunication Union (2018) *Measuring the Information Society Report 2018 - Volume 1. Geneva, Switzerland., ITU Publications*. Available at: https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR-2018-Vol-1-E.pdf.

International Telecommunication Union (2018) *Global Cybersecurity Index (GCI), ITU Report*. DOI: 10.1111/j.1745-4514.2008.00161. x.

Kerravala, Z. (2016) *Broadband Wan: The Importance of Setting Network Baselines*. [Online] Available at: http://blog.silver-peak.com/the-importance-of-setting-network-baselines [Accessed 10 May 2020].

Kreicberga, G. (2017) I*nternal Threat to Information Security-Countermeasures and human factor within SME. Kirun*a: Lulea University of Technology.

Kumar, D. A. (2017). *A Study on ISO 9001 Quality Management System: Reason behind the failure of ISO Certified Organizations*. Global Journal of Management and Business Research, Vol. XI (XI), 43-50.

Kumar & Ranjit (2005) *Research Methodology a Step – by – Step Guide for Beginners*, (2nd Edition), Singapore, Pearson Education.

Kundy, E. D & Lyimo, B. J. (2019) Cyber Security Threats in Higher Learning Institutions in Tanzania, A Case of University of Arusha and Tumaini University Makumira. *Olva Academy – School of Researchers*, Vol. 2, Issue 3.

Leder, F. (2016) *Proactive Botnet Countermeasures an Offensive Approach. Bonn: Institute of Computer Science IV*, Germany, University of Bonn

Lillis, D. *et al.* (2016) 'Current Challenges and Future Research Areas for Digital Forensic Investigation', in *The 11th ADFSL Conference on Digital Forensics, Security and Law (CDFSL 2016), Daytona Beach, Florida, USA, May 2016*. Available at: http://arxiv.org/abs/1604.03850 (Accessed: 6 October 2020).

Lubua, E., and Pretorius, P. (2019) 'Cyber-security Policy Framework and Procedural Compliance in Public Organizations', *Proceedings of the International Conference on Industrial Engineering and Operations Management Pilsen, Czech Republic, July 23-26, 2019*

Makumbi et al. (2018) *An Analysis of Information Technology (IT) Security Practices: A Case Study of Kenyan Small and Medium Enterprises (SMEs) in the Financial Sector*, Nairobi, University of Nairobi

Matandiko, K. (2017) 'Wahalifu wa kimtandao wavamia tovuti ya Chuo Kikuu Huria', *Daily Nation*, 24 October.

Mugenda.O.M & Mugenda. A.G (2003) *"Research Methods: Quantitative & Qualitative Approaches";* Nairobi, African Centre for Technology Studies (ACTS)

Myers, M. D. (2013) *Qualitative Research in Business and Management*, 2nd ed., London, Sage Publications.

Ministry of Works Transport & Communication (2016) 'National Information and Communications Technology Policy', *National Information and Communications Technology Policy*, (May).

Naden, C. (2019) *Stronger data protection with updated guidelines on assessing information security controls*. Available at: https://www.iso.org/news/ref2367.html (Accessed: 5 March 2020).

National Audit Office of Tanzania (2020) *General Audit Reports | National Audit office of Tanzania (NAOT)*. [Online]Available at https://www.nao.go.tz/index.php/reports/category/general-audit-reports (Accessed: 23 September 2020).

NIS (2018) *Framework for Improving Critical Infrastructure Cybersecurity*. [Online] Available at: https://nvpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [Accessed 10 March 2020].

Njiru, N. (2016) A *Framework to Guide Information Security Initiatives for Banking Information Systems*, Nairobi, Kenyan Banking Sector Case Study

Nyamongo, V. (2015) *Information Systems Security Management a Case Study of Private Chartered Universities in Kenya*, Nairobi, Strathmore University

O'Neill, P. F. (2016) *Building Resilience Through Risk Analysis. In: Resilience and Risk: Methods and Application in Environment, Cyber, and Social Domains* Azores: Springer, pp.451-468.

Sithole, T. (2019) *Assessing Cybersecurity Preparedness of Public Sector Information Systems. Pretoria*. [Online] Available at < https://repository.up.ac.za/bitstream/handle/2263/72687/Sithole_Assessing_2019.pdf?sequence=1 > [Accessed: 5 March 2020].

Tenable Network Security (2013) *Continuous Network Monitoring: Eliminate periodic assessment processes that expose security and compliance programs to failure*, Available at < https://docplayer.net/8634178-Continuous-network-monitoring.html > [Accessed: 5 March 2020]

Tanzania Communications Regulatory Authority (2020) *Publications & Statistics › Research Papers*, available at < https://www.tcra.go.tz/publication-and-statistics/studies-research-papers > [Accessed 21 April 2020]

Tanzania Commission for Universities (2020) *Universities Information Management System*, Available at: <http://uims.tcu.go.tz/> [Accessed: 14 March 2020].

Tanzania Commission for Universities (2018) *Higher education student's admission, enrolment and graduation statistics 2012/13 - 2017/18*, Available at: <https://www.tcu.go.tz/sites/default/files/Admission and Graduation Statistics.pdf > [Accessed: 6 March 2020].

Tanzania Computer Emergency Response Team (2020) *Reports – Tanzania Computer Emergency Response Team*, Available at: https://www.tzcert.go.tz/resources-2/reports/ [Accessed: 16 October 2020].

Zegers, N. (2016) *A Methodology for Improving Information Security Incident Identification and Response*, Rotterdam, Erasmus Universiteit Rotterdam.

Zwilling, Lesjak, D., Natek, S., Phusavat, K., & Anussornnitisarn, P., M. (2019) 'How to Deal with the Awareness of Cyber Hazards and Security in (Higher) Education?', *International Conference on Innovation and Management*, (August), pp. 433–439.