NETWORK SECURITY MODEL FOR UNIVERSITY NETWORKS IN KENYA

BY

JEREMIAH OYANA OWANGO

A Research Thesis Submitted to the Board of Post Graduate Studies in Partial Fulfillment of the Requirements for the Award of a Master of Science Degree in Information Security and Audit from Jaramogi Oginga Odinga University of Science and Technology

NOVEMBER 2023

DECLARATION AND APPROVAL

Declaration

This proposal is my original work and has not been presented for an award of a degree or diploma in any other university or institution.

Signature..... Date.....

Jeremiah Oyana Owango

I152/4056/2014

Approval

Supervisors

This thesis has been submitted for examination with our approval as university supervisors

Signature……. Date……..

Dr. Samuel Liyala

School of Informatics and Innovative Systems

Jaramogi Oginga Odinga University of Science and Technology

Signature……. Date…….

Prof. Anthony Rodrigues

School of Informatics and Innovative Systems

Jaramogi Oginga Odinga University of Science and Technology

Acknowledgements

I wish to present my special thanks to my wife for the encouragement she gave me, my mother for the undying support, I would also like to show my gratitude to my supervisors Dr. Samuel Liyala and Prof. Anthony Rodrigues for their assistance and guidance and without whom it was impossible to accomplish the end task, the SIIS lectures in Jaramogi Oginga Odinga University of science and technology for assistance rendered in carrying out the study and would also like to thank all those whose assistance provided to be a milestone in the accomplishment of my end goal. However, all those who assisted in this thesis completion are exonerated from errors or mistakes that maybe contained in the thesis.

Abstract

University networks contain a variety of information that varies from highly lucrative patents to personal information. The purpose of this study was to develop a secure network model that will enhance network security for the institutions in the country. The study objectively seeks to determine the existing network models and network security model and assess their weaknesses, it also seeks to establish what hinders implementation of network security in these institutions. The content scope of the study includes 51 chartered universities in Kenya, ICT technical personnel responsible for managing network assets, resources and services were the respondents and the study was carried out over a period of one year. The study adopted a descriptive research design, the study utilized the five point Likert scale in designing questionnaires. Purposive sampling of the respondents in the study was carried out in the study due to the fact specific ICT personnel in the institutions could answer the questions. Out of the population of 51 institutions a sample size of 49 institutions was got from the use of normal approximation to the hyper geometric distribution. 255 questionnaires were sent out, with each institution having 5 questionnaires sent to it. Secondary data on SWOT analysis of network models and network security models were described, frequency and percentages of general characteristics of respondents were described then correlation analysis was carried out to determine the relationship of the variables used in the proposed model, then a regression analysis was performed. It was established network security models have flaws that needed addressing. The outcome of the research is a binary logistic regression equation model that was used to predict the network security status of university networks based on the implementation of the protection, detection, response and recovery mechanisms. The security model developed will assist universities to effectively implement security measures in their institutions so as to protect networks infrastructure. It is the researcher's recommendation that training of staff on network security helps technical staff to have confidence in the network they are administering, so they are able to manage network-breaches in real time instead of reacting to attacks and also helps alleviate minor mistakes during normal work operations.

Table of Contents

List of Tables

List of Figures

Acronyms/Abbreviations/Symbols

BYOD	Bring Your Own Device
CAK	Communication Authority of Kenya
CCK	Communication Commission of Kenya
CDN	Content Distribution Network
CUE	Commission of University Education
CIO	Chief Information Officer
CIRT-CC	Computer Incidence Response Team- Coordination Center
CSIS	Center for Strategic and International Studies
DNS	Domain Name Services
DDoS	Distributed-denial-of-service
DNS	Domain Name System
GCHQ	Government Communication Headquarters
GoK	Government of Kenya
GEA	Government Enterprise Architecture
KE-CERT/CC	Kenya Computer Emergency Response Team
KE-CIRT	Kenya Computer Incident Response team
KENET	Kenya Education Network Trust
MFA	Multi-factor Authentication
NIST	National Institute of Standards and Technology
NREN	National Research and Education Network
OEM	Original Equipment Manufacturer

CHAPTER ONE
INTRODUCTION

1.1 Background Information

(Bechkoum, 2020) article network threats increasing for universities under lockdown, notes that the onset of the COVID 19 pandemic and the thereafter effect of national lock down, made millions of university staff and students migrated to remote learning in the space of a few weeks. Laptops and other Bring Your Own Device (BYOD) devices were bought and configured in a rush; cloud, Software As A Service (SaaS) was rapidly set up or scaled up, with security considered as an afterthought out of sheer urgency of getting services up and running, with many of these platforms remaining in place for the new academic year, this was also echoed by (Sawahel, 2020)

According to Right Privacy Clearing House, networks attacks to institutions of higher learning are growing annually and exponentially, while survivability of affected institutions and getting their infrastructure back online takes longer and longer (Rajaraman, 2014)

Symantec's global Internet Survey Threat Report (ISTR) has indicated since 2014 institutions of higher learning have maintained the top six most attacked entities in the global arena, this evidenced by the annual cyber security reports by ISTR (Symantec, 2014), Centre for Strategic and International Studies (CSIS), (CSIS, 2017) and Statista that have carried out surveys on network security status in universities. This trend has also been noted by (Symantec, 2016; Kenya Cyber Security Report 2019; MUIRURI, 2019; Johnson, 2021).

Joint Information Systems Committee (JISC) pointed out half of United Kingdom (UK) higher education institutions have been victims of wide spread networks attacks, with the increased remote working factored in, it is expected higher education institutions will become more liable for data breaches (Chapman, J., 2019). This is no different in East African universities, (Wasonga, 2019) noted that three of the largest universities in Kenya had their network compromised by the WannaCry global computer network epidemic in 2017. Chinese universities were not left untouched, 60 Chinese universities being hardest hit in academia, affecting staff and students, with some entire university services grinding to a halt, with 30,000 computers affected in a single Chinese institution, (Hatton, 2017; Lessing, 2020). This has been of great concern since the COVID 19 pandemic hit, as large portions of universities have adopted remote teaching technologies (Sawahel, 2020).

(BBC, 2019) reported REvil ransomware as the leading higher education network threat in the United Kingdom, following a spate of ransomware attacks to institutions of higher learning which include Newcastle, Northumbria universities and higher education colleges in Yorkshire and Lancashire bearing the brunt of the attacks. The Government Communication Headquarters (GCHQ) affirming it took months to restore services after the attack (Coughlan, 2020). Blackbauda a managed service cloud provider favored by universities and nonprofit organizations was compromised having core network equipment hijacked using zero day exploits that affected at least 19 universities from United Kingdom, United States of America and Canada (Tidy, 2020).

The education industry is ranked last in cyber security preparedness out of 17 major industries (CSIS, 2021), this is evidenced by a study carried out between April 2018 to October 2018 on 2,393 organizations with a minimum of 100 IP addresses accessing higher education networks, results indicated higher education industry is the lowest cyber security performer compared to other major industries, which performed particularly poorly in patching cadence, application security and network security, (Lee, 2020) in the article security threats affecting universities; highlighted this too.

Institutions of higher learning are increasingly being targeted by cyber-criminals, managing network threats in universities is problematic, due to the valued openness of their networks, the features that help universities to collaborate and thrive, such as open, information-rich websites, ubiquitous connectivity and collaborative platforms for students and staff leave them particularly vulnerable to network threats (Lee, 2020). It was also noted majority of universities lack business continuity plans, in addition the ECAR study, Shelter from the Storm: IT and Business Continuity in Higher Education (Educause, 2021) acknowledge that most business continuity plans at higher education institutions are not even tested, this was also a point of concern to (Pirani &Yanosky, 2007; Jorrigala, 2017; REMS, 2017), an indication it is a recurring issue.

This has been noted especially with the increased and successful ransomware attacks and network breaches in universities since the COVID 19 pandemic national lock down was initiated in economies globally that resulted in a rapid move to online teaching and learning as a means to curtail the spread of COVID 19 (Sawahel, 2020)

America's research universities are among the most open and robust centers of information exchange in the world, that are increasingly coming under network attack, most of it thought to

originate from China. Campuses are being forced to tighten security, constrict their culture of openness and try to determine unauthorized access to their networks. Universities and their professors are awarded thousands of patents each year, some with vast potential value, in fields as disparate as prescription drugs, computer chips, fuel cells, aircraft and medical devices which provide lucrative price for cyber criminals (Pérez-Peña, 2013; Lynn, 2018).

New Jersey based Rutgers University's internet services had been a victim of targeted attrition attack between 2013 and 2016 and large portions of its network was offline after the attacks, the university did not disclose which campus networks were affected or compromised but the institution however had to restrict all traffic to and from the internet disrupting the institutions operations (Coleman, 2015).

In 2013 Pennsylvania State University's College of Engineering revealed that it had been the target of two cutting edge network attacks between 2011 and 2013 that brought the institutional services to its knees that took several days to rectify. The network had to be put offline for three days to set up robust scanning and computer security protocols to take a proactive and aggressive stance towards future attempted intrusions, which revealed two more attacks against the College of Liberal Arts (The New York Times, 2013), the university admitted to fending off more than 22 million network intrusions a day (Perlroth, 2015).

In 2014 Penn State University's entire Engineering School had to be taken offline for an extensive investigation and clean-up of its network and systems due to infiltration of the institutions network (Cenzic, 2014), statistics reveal that from 2006 through 2013, over 500 universities in the United States reported network breaches. According to information from the database maintained by Privacy Rights Clearinghouse on data breaches, 30 educational institutions in North America experienced networks breaches between 2014 and 2018. Five of the thirty institutions actually had larger network breaches than the notorious Sony Hack with the shortest recovery time being 72 hours after putting affected networks offline (McCarthy, 2018). Between 2014 and 2016 the number of successful network attacks not only rose significantly but breaches became more aggressive and advanced, with frequency of security breaches affecting universities multiplied almost ten times (Verizon, 2016), by 2017 the number of attacks grew to 393 in an hour (in 2012 there only 5). In 2018 over 300 universities were victims of a giant network attack organized by Iranian hackers, with official information confirming 31 Terabytes of valuable intellectual property and data was

exposed (EDGUARDS, 2018; Lynn, 2018) with cybercriminals exploiting the weakness in human nature to infiltrate institutions (Verizon, n.d.)

(Harris &Hammargren, 2016) Breaches into networks at the University of California, Los Angeles (UCLA), University of Southern California and University of Maryland crippled university services leaving staff and students stranded and unable to access online services. UCLA health computers were also affected with disruption to access personal data of staff members and students; this attack was confirmed by the Federal Bureau of Investigation (FBI) and was still under investigation (KERR, 2018).

Canadian Universities were targets of sophisticated network attacks in 2016 The University of Calgary was forced to pay a $ 20,000 ransom following a ransomware attack on its core network equipment that affected a specific microprocessor, in 2019 University of Waterloo had a concentrated Sybil attack campaign trying to access its core switches and in 2020, The University of Saskatchewan was hit by a Denial-of-Service Attack (DoS) attack incapacitating its networks services (Ryerson University, 2019; Nicol, 2020)

Oxford University confirmed that its network security had been compromised by a network attack, totally crippling its data center by a Distributed Denial of Service (DDoS), (Brewster, 2012). The attack came a day after the disruption at Cambridge University's network; the institution had problems managing due to the sheer number of attempted breaches. After the breach in Oxford University was managed, hackers again gained access to the network and accessed a load balancing server in the physics department (universityworldnews, 2012). British Universities are being hit by hundreds of successful networks attacks each year, with more than 1,152 intrusions into British universities a day between 2016 - 2017. Ransomware, phishing and denial of service had been employed against universities, with affected universities being Oxford, Warwick and university college London (Bennett, 2017; Clatot, 2017; Oxford-Mail, 2017)

In Saudi Arabia (Alharbi & Tassaddiq, 2021) noted network breaches occurred in universities in the country due to lack of knowledge from students. Student Bring Your Own Devices (BYOD) are hijacked and used by hackers as an access point to gain unauthorized access to the institution’s networks. (Broadhurst & Chang, 2016) in the study cybercrime in Asian Universities; trends and challenges noted a similar pattern where intrusion to institution networks occurred through student BYOD eavesdropping, this was particularly rampant in India, Bangladesh, China and Japan.

90% of African universities are operating below the cyber security threshold, ie the point at which an organization cannot protect itself effectively (Muchira, 2018) this is evident in Kenyan Universities with most institutions affected by the REvil and Wannacryrasnsomware that crippled their networks (Muendo, 2019).

Between 2005 and 2015, higher education institutions in Kenya had been the victims of 539 network breaches. This trend was due, in part, to the sheer number of personal records kept by these institutions, considering their ever-changing student bodies, as well as the valued open, collaborative environment of most colleges and universities (Harris & Hammargren, 2016), this is echoed by (CAK, 2019; Lee, 2020) which also noted attackers would target university network segments that hosted servers that would host Intellectual Property of research in universities.

Weak internal and external IT security systems highly expose local universities to hacker collectives, (Ochieng, 2014). Kenya has experienced increase in network attacks since connecting to the global network of fiber optic cables, with institutions of higher learning suffering the brunt of the breaches (muiruri, 2019).

According to (Daily Nation, 2014) 72 university network resources were hijacked by hacker collectives originating from Russia by capitalizing on a flaw in the kernel of the operating systems that ran core network equipment in the institutions. Restoration of network services ranged from between 24 hours to 96 hours, this was of concern, especially since these networks serve gateways to university portals (Kimani et al., 2014). This was noted as a point of concern by (muiruri, 2019) identifying hacker collectives targeting university networks are now within the countries geographical boundaries.

A Cyberoam report places Kenyan Universities among African universities leading in network attacks, after Egypt, Morocco and South Africa (Business Today, 2015) implying students maybe a weak link in securing institutional networks. Most African universities are migrating most of their core services to the cloud in order to make processes faster and easier and to try and manage their security foot print (Standard Group PLC, 2020).

In 2016 a University of Nairobi Campus network segment was hit by REVIL ransomware where hackers then demanded a ransom of 10-bit coins lest the institution gets an escalated form of the attack to its core systems, the Communications Authority of Kenya (CAK) took over the matter and was working towards resolving the issue (Kajilwa, 2016), this trend of numerous successful

unauthorized network intrusions into universities is concerning. (Aineah, 2019) article on Student hackers: Exposing varsities vulnerable systems; where a student launched a legal fight against Kenyatta University after receiving discontinuation letter on suspicion of hacking into university core systems. The fact that KU admitted to students gaining unauthorized access to its network in open court raises questions of such cases that go undetected and unreported. This case brought to the lime light cyber security status in local universities; this was further confirmed by (Munguti, 2020) in a case where 2 Information Technology (IT) students from JKUAT were arrested for unauthorized network intrusions but in both cases the institution could not prove how the network intrusion occurred.

1.2 Statement of the Problem

According to studies carried out by (Aineah, 2019; Wasonga, 2019; Munguti 2020) indications of securing university networks in Kenya has proved problematic, this evidenced by the inherent weakness of network models and the successful network breaches documented and admission of rampant network breaches during litigation between universities and individuals over unauthorized network access. A number of efforts have been put in place to curtail the rampant number of network breaches but none is yielding positive results. There have been some attempts made to improve security of university networks in The United Kingdom and United States of America by use of a proprietary model and security equipment. It was noted the financial implication is quite significant (Bongiovanni, 2019; Miller, 2022) This would be problematic to achieve considering the limited ICT budgets in Kenyan universities. A solution to this problem is to develop a custom and cost effective network security model, which considers the network usage habits in the Kenyan university context and the dynamic security situation in these institutions which can be implemented using open source community edition software.

1.3 Objectives

The main objective of the study is to develop a network security model that comprises protection, detection, response and recovery measures to improve on security of university Networks.

The specific objectives include:

i. Analyse network models that are used in securing universities.

ii. Analyse the weaknesses that exist in network and network security models.

iii. Develop a network security model that integrates detection, response, recovery and protection that will help in securing universities network infrastructures.

1.4 Research Questions

The questions this research intends to answer are:

i. What network security models are used in university networks?

ii. What weaknesses exist in network and network security models?

iii. What network security model integrates detection, response, recovery and protection will secure universities network infrastructure?

1.5 Significance of the Study

It is noted network breaches in university networks continue to increase annually (Aineah, 2019; Wasonga, 2019; Munguti, 2020). A problem exists in that they are both prolific and increasing in complexity. Little work seems to have been done on the application of risk-based strategies involving network attacks in Kenyan universities; this research seeks to build an intellectual bridge between the resilient management of university network infrastructure and the applicability and adoption of network security strategies. Subsequently, this study examines the impediments of implementing and managing network security within a university environment and aims to understand how the environmental context, organizational complexity of a university and the many stakeholders which operate within it, influence the perception, implementation, needs and applicability of securing university network infrastructure.

1.6 Scope of Study

This study was carried out over a period of twelve months in Kenya; the target populations is 51 charted universities (CUE, 2015) in the country both public and private, by the use of normal approximation to the hypergeometric distribution (Morris, E., 2004), it generated a sample size of 49 universities. Respondents were selected from each sample size. The study covered the network security situation in universities in Kenya with focus being on network breaches as this the most rampant cyber threat affecting universities (Bradley, 2015; Maynard et al., 2020).

1.7 Assumptions

This study assumes the sample group has basic knowledge of data communication, routing and switching on large networks, network security and network attack traffic propagation, the basis of the assumption is based on university hiring techniques that provides mechanism that ensure hired personnel poses the academic and technical qualifications to hold the jobs required by the sample group. The study also assumes the institutions have set-up network and system monitoring services this assumption is based on the fact that the country's National Research and Education Network (NREN), Kenya Education Network Trust (KENET) provides best practices and training for member institutions on methods of managing and monitoring scalable networks and systems as a condition of membership to the NREN.

1.8 Definition of Terms

Bandwidth: amount of information that can be transmitted or processed through a wired or wireless connection

Computer Infrastructure: refers to the way a computer network is setup using different hardware and software.

Data Security: Process of protecting data from unauthorized access

Hacker: an entity that can gain unauthorized access other computers or networks

Organizational Culture: refers to the way student and staff behaves in academia, in access to information, research and teaching.

Network model: refers to a conceptual framework used to describe the functions of a data communication network.

Network Security Model: refers to a conceptual framework used to describe the functions securing a data communication network.

Network Security: refers to the protection of the underlying networking infrastructure from unauthorized access, misuse, or theft. It involves creating a secure infrastructure for devices, applications, users, and applications to work in a secure manner

CHAPTER TWO
LITERATURE REVIEW

2.1 Introduction

This section provides in-depth information relating to the research topic and similar studies carried out from the global arena to the localized one.

2.2 Overview of the Kenyan University Network Security Status

In Kenya Higher education sector comprises of public universities, private universities, Technical, Industrial Vocational and Entrepreneurship Training Institutions and Research and Development Institutions, but for this study we will refer to higher education institutions as universities. The Universities Act 2012 set up, The Commission of University Education (CUE) to plan for the establishment and development of higher education and training (Odhiambo, 2011). Commission of Higher Education (CUE) has authorized and given the letter of charter to 51 universities in Kenya, (Commission for University Education, 2020).

2.3 Characteristics of a secure network

Network security consist of provisions and policies adopted by a network administrator to monitor and prevent unauthorized access, modification of network resources, misuse or denial of computer network services (Pawar&Anuradha, 2015). According to (Kumar & Kumar, 2014) a secure network is any computer network with security measures that would prevent unauthorized access by ensuring confidentiality, integrity and availability of information on the network. Elaborating on this, for a network to be considered secure it must possess a form of health monitoring of devices on the network, traffic usage patterns (Pawar&Anuradha, 2015). Network security is important because it protects the integrity and privacy of sensitive information like personal identifiable numbers, financial information and intellectual property which happen to be in large amounts in universities. Unauthorized access, corruption or loss of this information would lead to loss of reputation and large fines imposed to the institution (Chapman, 2016; Kalniņš et al., 2017). Network security is also essential for protecting against malware and other kinds of malicious software that can damage computer systems and steal or corrupt information. Malware can be introduced to the network via email attachments infected websites and network vulnerabilities like misconfiguration, running equipment with known flaws and not upgrading to the latest firmware releases (Daya, n.d.).

2.4 Network Security Status in Universities

Universities in the country have not had a positive track record in securing their networks and information security assets; this is highlighted by (Aineah, 2019) in the article on Student hackers: Exposing varsities vulnerable networks; students hacking university networks was brought to the lime light by litigation between a student and Kenyatta University where the complainant argued active attacks were used by the defendant to gain access to the university network and access confidential student information. The demand for information security in institutions of higher learning has continued to rise since institutions of higher learning are seen as lucrative targets for cyber attackers, are not well secured and have already suffered multiple high impact network breaches, (Klovig Skelton, 2018; Sarraf, 2019).

The network threat landscape in universities consists of active and passive attacks:

Active attacks involve unauthorized change to a system, where an attacker tries to modify the content of a message for example:

1. **Spoofing:** An attacker attempts to use a network device to trick other computer networks by masquerading as a legitimate entity.
2. **Modification**: Involves modification of information in transit on the network examples include modification on routing table to reroute legitimate traffic to a rogue host (York, 2010)
3. **Wormhole**: An attacker records packets at one location in the network and tunnels them to another location (Hubaux et al., 2001).
4. **Fabrication**: Refers to attacks performed by generating false routing messages, such attacks are difficult to identify as the messages come as valid routing constructs (Hubaux et al., 2001).
5. **Denial of Services**: The attack aims at obstructing or limiting legitimate access to a certain resource. The resource could be a specific node, service or entire network (Aluvala et al., 2016).
6. **Sinkhole**: A compromised node tries to attract the data to it from all neighboring nodes, practically the node eaves drop on all the data being communicated on neighboring nodes (Aluvala et al., 2016).

7. **Sybil**: Attack where the reputation of a system is undermined by by creating a large number of pseudonymous identities and uses them to gain a disproportionately large influence on the network (Bhise & Kamble, 2016).

Passive attacks: Here the attacker does not interfere with routing or switching but monitors the information in transit, and tries to extract valuable information like node hierarchy and network topology. These attacks are difficult to detect as they do not involve any alteration of data.

According (FireEye, 2015) academia has published hundreds of thousands of papers on information security and network security yet in institutions of higher learning network security is left to technicians to fix with little to no facilitation from management boards. This is confirmed locally by (Aineah, 2019), during litigation between KU and one of its students, where it was noted the university management board did not have information on the institutions network security status and tasked the technicians to explain how a breach in the institution's network occurred, despite no investment on security being made in information and network security since 2012.

A review paper authored by (Chen & He, 2018) slightly differs where surveyed network risks in universities with relation to online learning has its findings primarily consisting of active technical attacks being a major technique to gain unauthorized access to university networks, as security is not given priority, indicating the researcher considered all forms of active technical attacks. The author noted the use of TCP/IP network model but subsequently fails to identify network breach mitigation techniques already in use in the institution due to the inherent weakness posed by the network stack, though recommends introduction of a dedicated computer network security model to help guide in information security implementation. (Maranga & Nelson, 2019) describes various techniques in which institutions of higher learning are attacked, the extent of the attacks and how the institutions can prepare to defend themselves, what is evident is the alarming frequency of attacks, the sheer number of network attacks originating both internally and externally to the institution. The author notes despite internationally available standards and procedures for securing enterprises in use, successful network attacks are on the rise not decline in institutions of higher education.

According to (Diaz et al, 2018) high levels of spoofing and phishing attacks to academic staff with an aim to access information relating to research data, intellectual property to staff routines and contacts. The author noted students were more prone to social engineering attacks, where attackers

attempt to gain access to the universities systems and networks using the student's BYODs devices then infect them so they act as zombies for use in DoS attacks either within the institution or externally. A review by (Cuchta et al., 2019) confirms phishing attacks being prevalent in universities targeting academic, finance and technical staff, the reviewer also noted fabrication attacks and social engineering attacks as a major attack vector in the university environment with emphasis on the human risk factor being identified as the culprit in gaining access to network resources. (Dadkhan et al., 2017) noted phishing attacks were being utilized by entrapping academic researchers into fraudulent call for papers which employ strategies to fool scholars where once a file is downloaded a malware installs on the don's system creating a backdoor to the university networks for the attackers.

(Liu et al., 2019) noted as much as network attacks are prevalent in North American universities the researchers noted a correlation between IT centralization and an increment in network breaches, where outsourcing, decentralizing and usage of cloud service providers of information resources are associated with fewer network breaches to an institution. The study was carried out over a span of four years and covered 505 higher education institutions. On the flipside it was noted centralized IT decision making as a key function of an institution made network attack breaches negligible as compared to institutions with non-centralized decision-making processes, with institutions with more complex and sophisticated network infrastructure benefitting more for centralized IT decision making. What was noted is phishing attacks and fabrication attacks were still of concern though the authors noted centralized IT decision making were associated with fewer breaches. According to (Custer, 2010) after an extensive theoretical analysis of network security assets and threats to those assets, notable identified network threats included passive attacks which include; traffic analysis, eaves dropping and foot printing typically carried out before a penetration test and active attacks which include; DoS, DDoS, spoofing, fabrication and modification. Authors (Ndiege&Okello, 2018) in their study information security awareness amongst students joining higher academic institutions in developing countries; evidence from Kenya noted the lack of information security knowledge in new students made them prime targets for social engineering attacks, they also noted most of the institutions under the study lacked standardized network security models that fit the institutions security situations, but rather adopted security models from other organization that do not address the types of network threats the particular institutions faced, they simply lifted a variety of models from elsewhere that were not even implemented in the original organization.

A study carried out by (Magutu et al., 2016) identifies the rise of network attack in the country since the fiber optic marine cable landing on the Kenyan coast; this was due to the readily available increased broadband bandwidth. Some of the highlighted network threats affecting higher education institutions include eavesdropping, spoofing, denial of service attacks, distributed denial of service attacks and rogue security software. The authors recommendation to limit or filter online access as form of securing end users would not work in higher education scenarios due to the valued openness and unrestricted access of information and collaborations within institutions and outside the institutions, the author also noted a basic structure underlying network security is required to be tailor made for institutions of higher learning that would assist in implementation of network security measures.

(Bongiovanni, 2019) presents literature regarding risk management frameworks and standards, information security policies, social ethical holistic approaches, technical solutions to network threats, cyber behavior, culture and awareness, and governance and how their usage in universities are critical in securing information in transit, the author discuses managing risks in institutions generally and not limited to network security, the author also discusses security culture and awareness in universities where it described new students and exchange student and staff as a weak link in network security as most do not comply or are not knowledgeable in security measures of respective institutions and tend to circumvent them by sharing of credentials, use of VPN, TOR browsers and the use of peer to peer sharing networks, the author finally concludes further studies need to be carried out that, to considers the unique culture available in universities machining it difficult to secure its networks.

The authors (Aguilar Quintero et al., 2019) evaluates network attack cases in South America where analysis is done of successful network breaches by use of technical methods to gain access to critical network systems, the study further noted the poor security implementation as a vector of attack by cyber miscreants as password sharing was rampant. A model was developed for evaluation of computer security for software products that were being purchased which emphasized on procurement of OEM (Original Equipment Manufacturer) software purchase, which simply managed one aspect of network security of protection mechanism, similarly a risk analysis model for network security was designed incorporating fuzzy decision theory but no literature exists on its implementation, and a network security model designed for solely securing financial business

computing assets. The authors identified inadequate access controls, weak policies and lack of training of technical staff and users.

2.5 Factors that hinder implementation of network security in universities.

Higher education will be used to refer to tasks carried out within academia and standard industry is any industry outside academia. Higher education institutions are struggling to find the nexus between the valued academic openness and securing their vast data networks.

Two important principles in higher education are academic freedom and valued openness; both are intrinsically present in universities. The purpose of academic freedom according to (Schaffer, 2014) is institutions of higher education are operated for the common good and not for the interest of either the lecturer or the institution, with common good reliant upon free search of truth and its free exposition. The precursor to the internet was university networks built for academics by academics without notion of the network threats and mistrust that currently plagues network users today. As the internet grew away from purely academic purposes, standard industry began seeing the benefits of the data networks and adopted it, cyber miscreants begun illegally accessing privately owned networks for personal gain, from this a vast and growing cyber security industry sprang to secure these networks to defend and protect against network threats and attacks, which standard industry quickly adopted but academia has been lagging in adoption of new security techniques and tactics. This is because universities draw intellectual growth from regular arrivals of visiting professors, students and other scholars and researchers from all over the world caring their BYODs requiring unfettered access to institutional network resources (Almaiah et al., 2020).

(Gil-Jaurena, 2013) explains, valued openness refers to the aspect of caring out teaching and research without any form of perceived obstruction technological or on social-cultural aspects, whether the function of teaching or research is being carried out within the specific institution or in collaboration with external institutional partners making securing networks of this kind of organization problematic. This is in contrast to standard industry where closed organizational data networks are valued in terms of organizational culture and security, the reason to this is it is easier to secure and manage closed organizational networks as emphasis is on securing of information and not sharing or collaborating. Developing security policies and guidelines specific to those industries for example banking can be achieved with little change if any to operational procedures. This methodology does not work on higher education networks due to the dislike of restriction or obstruction of information on data networks.

2.5.1 Uncontrollable networks

University student and faculty populations are massive, ranging from tens of thousands to hundreds of thousand users who access and use the institutional networks (Diesch et al., 2020). From on campus students, those accessing the network remotely, visiting scholars, collaboration partners all accessing the network around the clock, this is without even considering unauthorized users accessing the network, is a daunting task when it comes to securing university networks(Li, 2017). In an age of Internet of Things (IoT) students now use tablets 61%, smart devices at 27% and 25% gaming consoles on university networks (Maple, 2017), university network security is no longer about securing personal computers utilizing network services, but a vast range of network ready devices.

With most university campuses being decentralized, with individual departments and research groups often managing their own data and information technology assets it's not simple keeping track of where all the sensitive information is stored and what is going on across the entire network (Pandey, 2016), this aspect of decentralized management of network resources makes securing institutional networks problematic

2.5.2 Poor Network Practices and Outdated Security Measures

Lack of education on network security best practices is a major contribution to poor security hygiene from students and faculty, (Maple, 2017) noted 60% of faculty and staff do not make any network security changes but leave default security measures on their devices, while 57% use out of network security mechanisms. This not unique to staff as it's been recorded 25% of students access the network with malware on their BYODs (Maple, 2017). Certain network physical segments run legacy network devices with known vulnerabilities, which are used as a stepping stone by attackers to gain access to the entire network or launching pad to attack other networks (Perlroth, 2013)

With the embrace of digital transformation since the COVID pandemic users have become more device reliant making university networks more complex and difficult to manage (Sawahel, 2020).

2.5.3 Higher Education Security Varies across the Globe

UK universities had a 92% confidence in their students and faculty members securing personal IT resources, while in Germany75% of university network users said they did not feel their personal devices were secure while on campus networks, while in the United States ICT teams felt only 47% of students were taking necessary steps in securing their BYODs, (Barlette et al., 2021).

Academic freedom and openness being tenets of higher education provide a glimpse of the complexity in securing information and networks, according to (Yilmaz & Yalman, 2016), the valued free flow of workforce and annual rotations of new students, guest and employees also adds to the universities network security challenges. Even though institutions of higher learning face ever increasing network attacks that increase exponentially annually the initiative of implementing network security varies greatly (FireEye, 2015; UNIT, 2019). There are organization culture issues in universities such as valued academic freedom, free flow of information, ease of access of information to collaboration partners within and outside the university, an ever changing large number of staff and student body, highly technically competent networks end users, interconnectivity of university campus dispersed over a large geographical area with equipment that range from state of the art to legacy systems and various ad hoc networks managed by independent sections within the university is not typical in standard nonacademic organizations, are security challenges that make it difficult to secure network resources and assets in universities (Adams & Blanford, 2003; Ncube & Garrison, 2010; REMS, 2017; Ryerson University, 2019; Almaiah et al., 2020).

2.6 Weakness in Network Models

The OSI Model and the TCP/IP model are today the de facto network models used in enterprise networks, with TCP/IP model taking 80% adoption of the networks on the internet; they both have their strengths and weaknesses (Hartpence, 2013).

2.6.1 Open Systems Interconnect (OSI)

Development of the OSI model began in 1977 by the International Organization for Standardization (ISO); it is simply a conceptual framework that can be used to understand network communication. This model has been used since 1983 to teach and guide networking basics and to troubleshoot networking issues. It's so influential in network development that most network communication protocols in use today have a structure that is based on the OSI. As reliable as the OSI is, their lacks a standard that all network security professionals can adhere to (Blackfield & Bambernek, 2021). This model's benefit is it acts as a guidance tool to develop a desired network model as it is generic, it's a layered model where changes in one layer does not affect the next layer, its flexible in nature as it separates, services, interfaces and protocols, standardization of protocols and it supports connection and connectionless oriented services (Kumar & Dhanda, 2017)

The weakness this model presents is; it tends to be broad and does not provide a form of security implementation for enterprise networks, OSI criteria are theoretical and do not provide satisfactory clarifications for practical network security, it's merely a theoretical concept it lacks consideration of accessibility of appropriate technologies, hence its practical applications are limited (Rao & Nayak, 2014).

2.6.2 Transport Communication Protocol/ Internet Protocol (TCP/IP)

Designed in 1970 by the Defense Advanced Research Project Agency (DARPA) scientists, it provides end-to-end data communication providing specifics on how data should be transmitted, addressed, packetized, routed and ultimately received. It Involves four layers namely application, transport, internet and link-layers, according to (Ravali, 2014) the TCP/IP suite has strengths of cross platform communication among heterogeneous networks, it's an industry standard, it's not owned by any entity, it enables scalable client-server architecture and assigns IP addresses on computers regardless of the platform making it identifiable over the network.

TCP/IP suite has many design weaknesses as far as security and privacy are concerned, this is probably due to the fact when the suite was developed in 1970 network attacks were not prevalent. The flaws present in many implementations make a bad situation worse, cyber-criminals capitalize on weaknesses in the TCP/IP suite to gain access to institutional networks (Mateti, 2007); the attacks that capitalize on the TCP/IP suite weakness include;

1. **Buffer overflows**; if an attacker is knowledgeable in the layout of a program one can intentionally feed output to the buffer locations that the buffer cannot store, over writing areas holding executable code and point the program to an infected payload. Services affected are DNS bind service, KOHA library system; send mail and IIS services which are heavily utilized in university networks (Hunt, 2002).
2. **Route table poisoning**; network services are map implemented as table look ups, which are dynamic with update methods well defined, but how to define updates and how they implemented are ill defined leaving an opening for malicious actors to tamper with the tables, poisoning it (Hunt, 2002).
3. **Illegal packets**; packets with the unexpected tag in some fields are illegal as a legitimate sender could not have constructed them. Receiving end software ought to check on such

packets but RFCs were ambiguous and legacy software developers not cautious (Hunt, 2002).

4. **Storms**; these are unusually high number of packets, for example when flood ping is utilized which can also create a denial of services, if the storm is persistent (Hunt, 2002).
5. **Denial of service (DoS)**; the goal of DoS is denied legitimate users from accessing a network resource, by flooding the resource with illegitimate traffic (Hunt, 2002).
6. **Finger printing a system**; an attacker scanning a LAN to identify what services are running, then scanning systems that provide those services to identify the operating system, as operating system vulnerabilities are specific to particular operating systems and can be capitalized on or software running, the process also creates illegal packets (Hunt, 2002)

(AT&T, 2015) also noted the suite has a series of inherent flaws in the protocols that act as enablers to the vulnerabilities mentioned above, it was designed to be implemented on Wide Area Networks (WAN), it is not optimized for Local Area Network (LAN), it's not generic in nature and cannot describe connections like Bluetooth.

2.7 Identification of Network Security models

Network Security is defined as specializations in provisions and policies to prevent, monitor and audit unauthorized access, misuse, modification and ensuring computer resources are available through proper procedures (Kumar & Kumar, 2014). Technical personnel transitioning to positions that were previously held by other network security personnel, learning what security mechanisms have been implemented and what has not can be a daunting task. To secure university networks that consist of a mix of different network architectures, uses and security implementation requires a template that can be used and tweaked to improve security status of an institution; this is where a model is utilized.

2.7.1 Network Access Security Model (NASM)

This model reflects the general plan and policy of ensuring network security, this model addresses technological weakness; addresses intrinsic security weaknesses in network technologies like the TCP/IP stack and OSI stack. Configuration weakness; involves identification of weaknesses in network configurations and correctly configure network devices to compensate for the error in configuration and security policy weakness; create unforeseen security threats. The network may

pose security risk to itself if users do not follow set security policy (Xu et al., 2019). This model has seven layers, which are an amalgamation of the OSI and TCP/IP network model:

1. **Physical layer**: Involves organization of the physical security of network equipment for example CCTV, fire suppression systems.
2. **VLAN Layer**: Virtual segmenting a network based on certain classifications for security purposes.
3. **ACL Layer**: Creation and maintenance of access control lists which allow or deny access between hosts on similar or dissimilar networks.
4. **Software Layer**: Helps protect user layer and ensures software validity.
5. **User Layer**: Involves user training of the security of the network
6. **Administrative Layer**: Informs on training of administrative users
7. **IT Department Layer**: This layer contains all the network security professionals responsible for securing the network.

2.7.2 Network Security Model (NSM)

According to (Abdulghani, 2009), this model informs how information is transferred over an insecure network, the security model ensures both the sender and receiver must mutually agree to communicate and share messages; a mutually agreed communication channel is used for an established communication. The information transmitted is encrypted using an agreed technique at the sender and decrypted at the recipient's end. A trusted third party is required to transmit the information through the insecure channel for the two parties involved in the communication. (Jang-Jaccard & Nepal, 2018) notes the weakness this model possess is, it is generalist and its implementation covers a wide range of industries. It is more of a general security template that was designed for Wide Area Network (WAN) communication. For Local Area Networks (LAN) usage over heads in decryption and use of a third-party transmission provider causes increase in costs and delays in communication. (Khan, 2017) further notes the model does not put into account the complexity involved in implementing the security model and the reliance on a third party to ensure message is transmitted securely make an organization not self-reliant.

2.7.3 Privacy Preserving Demand Response (P2DR) Model

(Xu et al., 2019) notes the classic adaptive protection model P2DR propose a security capability consisting of protection, detection, response and recovery mechanisms centered on policy, however

networks with the mentioned security capabilities and phases are passively protected lacking sufficient ability to detect threats in advance to proactively defend against them.

The P2DR model was not exclusively developed with data communication in mind; it was developed for general critical infrastructure including power grids, sanitation systems and telecommunication systems and not dedicated to computer networks. (Kullgren, 2019) noted its major strength is its adaptive nature in countering threats, which also brings out its major weakness as network threats are inherent in its protocol stacks and these were not put into consideration during the development of the model as it was not intended for data communication networks. This is especially critical in the university set up as a mix of legacy network systems operate in conjunction with cutting edge network systems; it does not address how to handle the security in decentralized management of ad hoc networks within a major network but can be used as a template to create model ideal for academia due to its malleable nature.

2.8 SWOT Analysis of Network Models and Network Security Models

The study scrutinizes SWOT analysis carried out by various researchers for the network model and network security model; SWOT analysis tables in Appendix 7.3:

According to (Costa, 1998; Danesh, 2021) the OSI model tends to be prescriptive, it provides a neutral networking environment so that computers from different manufacturers will be able to communicate effectively; the SWOT analysis on the model indicate weaknesses currently outweigh strengths of the model, but its opportunities; ability to redefine all the rules and standards in accordance with modern knowledge makes it an ideal model for use in developing frameworks with evolving models. The analysis of the model also notes, members of staff in organizations as a major threat on the model usage.

(Brittin et al., 1995; Forouzan, 2002) notes the TCP/IP model tends to be descriptive, SWOT analysis of the TCP/IP model indicates strengths of the model outweigh its weaknesses; its biggest strength is that each particular implementation can use operating system-dependent features, generally resulting in greater efficiency (fewer CPU cycles, more throughput for similar functions), while still ensuring interoperability with other services (Ravali, 2014). One of the weaknesses of the model is the fact it represents the model itself, it cannot be used in conjunction with other network models making it rigid and resistant to technological evolution. Threats to the model are the noted network threats the study is trying to address.

According to (Kizza et al., 2013) the Network Security Model is adequate for its time, the strength of the model's private key used in the encryption process is robustly resistant to brute force attacks, the secret key algorithm requires less computing power to be created, but its weakness is in the security of key exchanges which stands out as its major flaw. Opportunities to the model is increase in computational power will simply create larger encryption hashes, making it harder to crack the encryption hashes.

(Backfield & Bambernek, 2021) noted the Network Access Security Model was created to address and allow general information security in an organization and address the weakness in established network models, the model addresses most of the weaknesses in the OSI and TCP/IP model, its weakness is it lacks a monitoring aspect in network security which makes it a reactionary model.

(Liu et al., 2010) noted the P2DR model breaks down security into four manageable sections of protection, detection, response and recovery. It provides a template that can be improved on by adding organization security specifications and requirements. According to (Xu et al., 2019) the weakness of the model is an indirect strength as it leaves room for improvement of the model for a variety of industries. The opportunities this model provides makes it ideal in developing an inclusive model tailor made to the information security scope of universities as it is malleable to user requirements.

2.9 Developed network security model

The developed model utilizes the P2DR model as a template that subdivides the network security requirements into manageable domains of protection, detection, response and recovery. The model improves on the P2DR model and utilizes the strengths of the NASM and NSM; the two models which have been used extensively on data networks on the internet, but they all lack the detection aspect of security of data networks and little literature exists on their successful use in the university network environment, the developed model will capitalize on active network monitoring as a means to deter threats before they occur.

2.9.1 Protection

The goal of this phase is to reduce the attack surface for the potential intruder, by use of physical or logical measures before the attack affects the network. This phase includes strategies, processes and/or products designed to prevent the success of the attack (Cui et al., 2020).

2.9.2 Detection

The goal of this phase is to reduce the time to identify threats and attacks, which requires continuous and comprehensive monitoring of the network and use of sophisticated analytical tools that provide detection capabilities (Cui et al., 2020).

2.9.3 Response

This phase deals with discovered threats or attacks in a timely manner, it combines comprehensive investigation, evidence collection and traceability analysis to determine the scope and root course of the threat and appropriate countermeasure to be deployed (Cui et al., 2020).

2.9.4 Recovery

The goal of this phase is repairing the damage created by a successful attack in time to ensure the confidentiality, integrity and availability of the network services and resources. It includes data recovery and business recovery (Cui et al., 2020).

The NASM concentrates on data transmission through a public network by utilizing a trusted channel provider; it fails to address overheads in terms of cost, encryption and decryption or how to adapt to failures in LAN environments. The NSM on the other hand addresses short comings of the OSI and TCP/IP models by including security layers, which include Virtual Local Area Network (VLAN), Access Control Lists (ACL), software layer and the weak link on a network; user layer, administrative user and IT department layer. The model does not include a monitoring element in any of the security layers. The P2DR model is generic, it was not designed for computer or network security but has been generally adapted to network security in power generation industries, it broadly proposes how best to secure an enterprise network.

The proposed model will address the mentioned short coming by including an aspect of active monitoring of computer networks and protecting against breaches, this is achieved by utilizing Protection, Detection, Response, and Discovery mechanisms.

2.10 Conceptual framework

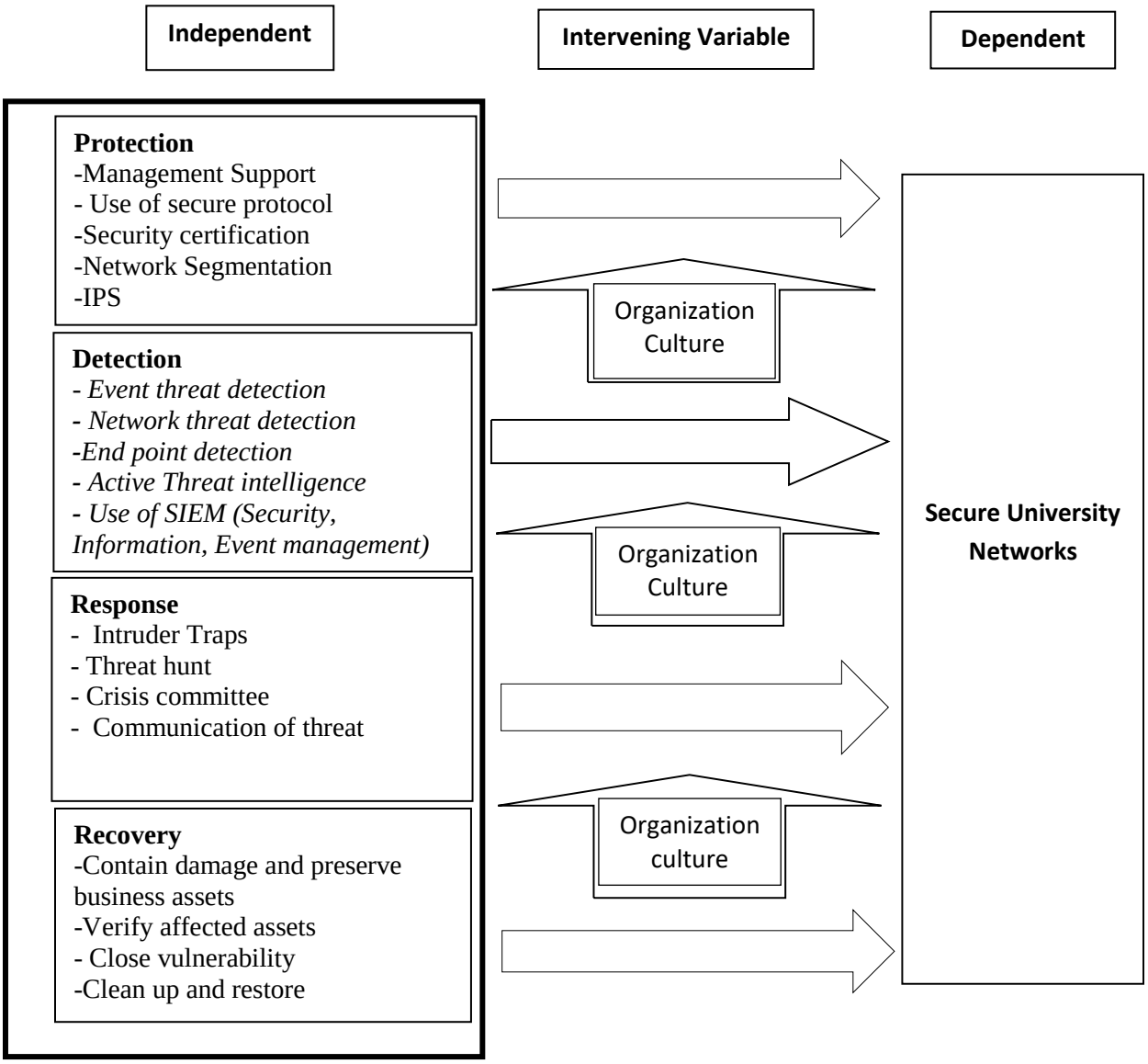


Figure 2.1: Conceptual Framework for the study

The conceptual frame-work shows the interaction between the different variables, secure university network is the dependent variable, while the independent variables are protection, detection, response and recovery.

The security infrastructure adopted by institutions depends on whether the type of security mechanism chosen will influence how network threats would affect an institutions information security network and the severity of attacks and how capable and efficiently an institution would

continue delivery of services at acceptable predefined levels following a disruptive incident (Tzenev et al., 2015)

2.11 Summary of Research Gap

Evidence on literature has shown institutions of higher learning are the top four most attacked entity by cyber criminals since 2010, (Lennon, 2010; Wagstaff & Sottile, 2015; Symantec, 2016; *Kenya Cyber Security Report 2019*; MUIRURI, 2019; Johnson, 2021) and the least secured in Kenya (Kaimba, A., 2018) with catastrophic effects. According to (Rahim, 2021) it is evident of scarcity of literature of network attacks of universities in developing nations. Literature identifies weaknesses in network security models that are used as guides in implementing network security in universities in Kenya. The Network Security Model (NSM) concentrates on point-to-point encryption and reliance on a trusted third party to manage the data transmission but it fails to address tracking and identify potential threats actively. The Network Access Security Model (NASM) addresses the protocol weaknesses inherent in network models, it addresses the weak link of the human aspect in network security, but the model lacks a layer that addresses intrusion detection. Literature on the P2DR model indicates the model was created as a general technical model, that has been used to secure power grids and Supervisory Control and Data Acquisition (SCADA) systems, literature exists on suggested use in securing of information technology assets but no literature exists on its use on securing network infrastructure. Although network security models exist none address the detection issue, the P2DR model provides the template but does not provide the guidelines on how to perform detection, this is the gap the study intends to address.

CHAPTER THREE
RESEARCH METHODOLOGY

3.1 Introduction.

This section describes the fact-finding methods for data collection, analysis, design tools and development that will be used to conduct and derive results from the study guided by the objectives

3.2 Location of the Study.

The study was carried out on fully charted universities in the Republic of Kenya which are numbered at 51 (Commission of University Education, 2020).

3.3 Research Design

This study adopted a descriptive research design, according to (Creswell, 2002; Kothari, 2004) the design is ideal as it allows the researcher identify characteristics in a study and describe how those characteristics affect the study by exploring of the correlation between two or more phenomena, in this case of this study protection, detection, response and recovery.

The study utilized survey method in data collection, according to (Ondersma et al., 2017) surveys are ideal as a useful and legitimate approach to research that has clear benefits in helping to describe variables and constructs of interest. Purposive sampling of the respondents in the study was carried out in which the participants filled questionnaires centered on the subject of interest. According to (Kelly et al., 2010) purposive sampling is used to select respondents that are most likely to yield appropriate and useful information, in this case ICT technical personnel.

3.4 Target Population.

The population of the study was 51 fully chartered universities in the country (Commission of University Education, 2020). The respondents included system administrators, network administrators, information system managers and security administrators. These respondents were chosen due to their frequent interaction with network systems and perceived technical and academic qualifications based on hiring practices in universities making them have a current knowledge of the security status of the network in the institutions.

3.5 Sample Size

To determine the sample size for small populations, a study uses the normal approximation to the hypergeometric (small population) distribution (Morris, 2015). The sample size of study was

determined by use of normal approximation to the hyper geometric distribution. According to (Collins & Morris, 2008) it suits the study as it is a discrete distribution that models the number of events in a fixed sample size when the total number of items in the population that the sample is known and the population size is small: The population of the study meets both requirements for use of the distribution.

$$n = \frac{NZ^2pq}{E^2(N-1)+Z^2pq}$$

$$\frac{N = NZ^2\,pq}{E^2\,(N\text{-}1) + Z^2pq}$$

Calculating sample size for small populations adopted from (Collins & Morris, 2008)

n = required sample size

N = population size

p and q = populations proportions value set for 0.5 (Collins & Morris, 2008)

Z = Value that specifies the level of confidence you want in your confidence interval when you analyze your data. Typical level of confidence for surveys is 95% in which case z is set to 1.96 (Collins & Morris, 2008)

E = Accuracy of sample proportions. Note for the sample proportions to be accurate E should not be lower than $^1/_n$ (Collins & Morris, 2008). Therefore, a value of {0.03} was used.

According to (Saunders et al, 2009) in most business and management researches, researcher's use 95% of to within plus or minus 5% of the true value of 1.96 when using 95% confidence. Using the above equation, the sample size of the research study was found to be 49 as shown below:

$$n = \frac{51_x\,1.96^2 \times 0.5 \times 0.5}{0.03^2\,(51\text{-}1) + 1.96^2 \times 0.5 \times 0.5}$$

$$n = \frac{51x3.8416x0.25}{0.0009(50) + 3.8416x0.25} = \frac{48.9804}{0.045 + 0.9604} = \frac{48.9804}{1.0054} = \frac{48.717}{1.0054} = 48.455 = 49$$

Forty-nine institutions were selected as the sample size; five respondents from each institution were chosen, according to (Shakoor & Abbas, 2021) adequate responses for analysis on a small sample size is achieved by using a multiplier of a minimum of 5, this done by taking the total questions in the questionnaire and multiplying by 5, in the case of the study 51 questions, giving 51*5 equals to 255, then divided by the number of sample size of 49, 255/49 = 5.20. Each institution in the sample size were assigned a minimum of 5 questionnaires. Questionnaires were given in excess to cater for non-responses and incomplete questionnaires. A total of 238 respondents had valid responses.

3.6 Sampling Techniques

Purposive sampling, a homogeneous non-probability sampling method is ideal for the study because it is characterized by a deliberate effort to gain representative samples from a specific knowledge domain with knowledgeable experts within that domain (Tongco, 2007), was used to select the respondents, whose inclusivity was based on the professional and academic qualification to manage networks and network systems, who were; network managers, network administrators, network technicians, database administrators, cyber security specialists, systems administrators and ICT officers. This was mainly aimed at people whose work is connected with aspects of network data transmission, storage and security. Purposive sampling is ideal for the study because specific staff members are knowledgeable in the institution's network security status.

3.7 Data Collection Instruments

(Forza, 2002) states various techniques that can be used to collect data from different sources in various settings. In this particular setting a user defined structured questionnaire was designed using a five-point Likert scale with responses for each statement recorded on a range of 0= strongly disagree, 1= Disagree while, 2 = Neutral, 3 = Agree and 4= strongly agree. The study utilized questionnaires to get responses from respondents, since the aim of the research was to solicit accurate and reliable data from selected respondents, coupled with in depth inquiries, closed ended questions featured in the questionnaire.

Data for the study was gathered through structured questionnaires that were sent to the respondents via Google forms. Digital questionnaires suited this study well since the targeted universities are geographically dispersed across the country. The questionnaires were presented in three sections, section one addressed general characteristics of the respondents and institutions, section two addressed questions related to the objectives of the study and section three addressed the questions

relating to the proposed security model which encompassed Protection, Detection, Response and Recovery.

The questionnaires were addressed to the ICT's technical team members who by virtue of being in charge of central universities IT infrastructure were in a position to respond adequately to questions on challenges inherent to network-security and restoration of services in the event of a catastrophic failure.

3.8 Validity and Reliability of instruments

3.8.1 Validity

According to (Golafshani, 2015), validity is the degree to which results obtained from the analysis of the data represents the phenomenon under study. Construct and content validity were utilized in the study. To ensure that the tools measure what they purport to or construct validity, a pilot study was carried out at Maseno University's three different campuses to analyze and ensure the consistency of the respondents. Content validity refers to whether the specified domain of content is actually measured. Content validity is best assessed by Subject Matter Experts (SMEs), or people thought to occupy higher levels of the construct being measured. Content validity of an instrument is improved through expert judgment (Readhead et al., 1996). As such, guidance was sought from the supervisors and other experts from the School of Informatics and Innovative Systems in Jaramogi Oginga Odinga University of Science and Technology, to facilitate improvement of content validity of the research instruments. The experts reviewed the items systematically in light of the intended construct, and rated the degree to which each item was relevant to the construct being measured. Content validity ratio was utilized to objectively gauge the content validity of items on an empirical measure: According to (Lawshe, 1975);

$$CVR = (2ng/N) - 1 \quad \text{..... eqn (2)}$$

$$= (2*5)/5\text{-}1 \qquad = (10/5)\text{-}1 \qquad = 2\text{-}1 \qquad = 1$$

Where ng = the number of institutions who think the item is good

And N = the total number of institutions.

CVR= Content Validity Ratio

Institutions rated the items on the questionnaire taking in consideration all types of validity. According to (Lawshe, 1975), a CVR of +1 indicate perfect agreement between the subject matter experts regarding the validity of content of the questionnaire.

3.8.2 Reliability

A measuring instrument considered reliable if it provides consistent and dependable results (Kothari, 2004). To ensure reliability, during the pilot study the test and retest method which involves the research tools being administered twice in a period of two weeks was carried out. This ensured consistency of respondents in giving their answers and also the short period ensured that nothing much had changed since the last administration.

The Cronbach's Alpha value was calculated using SPSS and a value of 0.790 as the table 3.1 indicates was presented. A total of 51 items were presented to respondents to give their opinions. Cronbach's Alpha provides an estimate of internal consistency of variation in the variables in the scale. (Charter, 1999; De Vellis, 2003) consider an alpha value of between 0.65-0.8 adequate for reliability testing, the scenario in this study also realizes a lower value of Cronbach's Alpha because of the variant areas of interest which should be included in the questionnaire to establish network security threats and vulnerabilities, implemented network security and suggested security.

Table 3. 1: Cronbach's alpha

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.790	.735	51

3.9 Data Collection Process

The researcher obtained permission for data collection from Jaramogi Oginga Odinga University of Science and Technology's School of Graduate Studies. The researcher also applied for a research permit form National Commission for Science, Technology and Innovation (NACOSTI). Once the permissions were granted, the researcher proceeded to collect data. The questionnaire was designed in-line with the objectives of the study. Structured questionnaires with four sections were used to collect data, because of the confidentiality of respondents and institutions institution and respondent names were not collected.

3.10 Data Analysis

A correlation analysis was done to establish the relationship between the dependent and independent variables. A logistic regression analysis is used because it is ideal in determining the probability of success or failure of the developed model and it is ideal for use to analyze close ended questions in a survey.

out to establish, the strength of relationship between the predictors and the predicted variables and the extent of that relationship. The outcome of the analysis was utilized in conceptualizing a model, which was used to come up with a model for the securing university networks.

3.11 Ethical Consideration

Before administration of questionnaires, the consent of participants was sought by first having a telephone call introducing the researcher and the study, then requesting the participant to take part in the study. During administration of the questionnaires a terms and conditions radio button had to be accepted before gaining access to the digital questionnaire that ensured informed consent and voluntary participation, that guaranteed confidentiality and anonymity by not collecting any personal information and communication of the result if desired by the participant. This ensured that participants felt free to disclose the information that they have. The participants were made aware what the study entailed and how the responses given would be used in helping in securing university networks and systems. Confidentiality of participants' feedback was censured by making the institutions in the sample size anonymous including the respondents. This allowed the participants to freely offer their ideas and information without fear of being victimized. A letter of research authorizing the collection of data was sought from Jaramogi Oginga Odinga University of Science and Technology to legalize the research.

CHAPTER FOUR
DATA COMPILATION, ANALYSIS AND PRESENTATION.

4.1 Introduction

The purpose of this study was to come up with an information security model for University networks in Kenya. In-order to achieve the main objective of the study data was collected from Information Technology (IT) professionals in these institutions by use of structured questionnaires. This chapter presents analyses and interprets the findings which will be presented in tables where appropriate. Frequency tables have been used to present the results with SD-Strongly Disagree, D-Disagree, N-Neutral, A-Agree and SA-Strongly Agree.

4.2 Respondents general characteristics

Table 4. 1: Employment Length of respondents

		Frequency	Percent	Valid Percent
Valid	6 months to 1 year	51	21.4	21.4
	1 to 3 years	106	44.5	44.5
	More than 3 years	81	34.0	34.0
	Total	238	100.0	100.0

Out 245 respondents, 238 respondents had valid responses. Table 4.1 indicates out of the 238 respondents the researcher noted a total of 21.4% of respondents have been in the employ of the institution for a maximum of 1 year, 44.5% have been in the employment of the University for a Maximum of 3 years and 34% have been in the employ of the institutions for over three years. This is good information as network security is based on learning network habits of users so as to better predict possible incursions or irregular usage on the networks to properly address the issue.

Table 4. 2: Student population in relation to technical personnel security certification

What is the Student Population of your institution? * Who handles IT security in your institution? Cross tabulation

Count

		Who handles IT security in your institution?				
		Network Administrator	Other	Security Specialist	System administrator	Total
What is the	Below 5,000	22	10	0	16	48

Student Population of your institution?	Between 5,000 - 15,000	70	15	27	35	147
	Over 15,000	27	0	6	10	43
Total		119	25	33	61	238

Table 4.2 indicates the ranges of student population in the institutions in relation to certification held by those who administer the networks. From the tabulation it is evident functionality is given precedence over security in the institutions, with network administration being given higher priority with a cumulative total of 119 of the respondents acknowledging that certificate is held by technical staff in their institutions, a cumulative total of 61 respondents acknowledge system administration certification was given precedence with security specialists trailing at cumulative total of 33 respondents. Employment of certified security personnel in universities is not emphasized; this is of concern considering most universities have migrated their systems to run on networks after the COVID pandemic, posing a great security risk.

Table 4. 3: Network Model usage

What network model is utilized in your institution?

		Frequency	Percent	Valid Percent
Valid	OSI Model	52	21.9	21.9
	TCP/IP Model	172	72.2	72.2
	Don't know	14	5.9	5.9
	Total	238	100.0	100.0

Table 4.3 indicates 72.2% of respondents acknowledged the TCP/IP model as the model of choice in their institutions, these respondents' preference was not based on knowledge of strengths or weaknesses of selected models but simply it's what was implemented in the institution by time of their employment.

Table 4. 4: Network Security Models usage

Does your institution use any of the network security models?

		Frequency	Percent	Valid Percent
Valid	Network Security Model (NSM)	79	33.2	33.2
	Network Access Security model (NASM)	87	36.6	36.6
	P2DR	2	.8	.8
	Don't know	70	29.4	29.4
	Total	238	100.0	100.0

Table 4.4 indicates the usage of network security models in universities with the NASM usage at 36.6% and closely followed by the NSM at 33.2%.

4.3 identification of network and network security models

Table 4. 5: Networks Security Model weakness

Network Security Model: Network Security Model (NSM)	SD %	D %	N %	A %	SA %
- Addresses external access to the internal secure network	26.32	13.16	60.52	-	-
- Addresses encryption of data transit	-	-	6.32	39.56	54.12
- Addresses firmware and network security patching	52.63	26.32	21.05	-	-
- Utilizes secure protocols e.g. VPN, IPSEC	-	-	15.79	44.74	39.47
- Emphasizes segmentation of the network	55.3	42.1	2.6	-	-
- Prioritize most critical network assets	50.82	10.2	38.98	-	-
Network Security Model: Network Access Security model (NASM)	SD %	D %	N %	A %	SA %
- Addresses external access to the internal secure network	50.0	12.12	20.63	10.1	7.15
- Addresses encryption of data transit	-	13.45	51.3	35.25	-
- Addresses firmware and network security patching	-	28.6	11.4	60.00	-
- Utilizes secure protocols e.g. VPN, IPSEC	26.31	23.16	10.53	-	40.00
- Emphasizes segmentation of the network	15.79	10.53	-	21.05	52.63
- Prioritize most critical network assets	39.47	5.27	-	15.79	39.47
Network Security Model: Privacy Preserving Demand Response (P2DR)	SD %	D %	N %	A %	SA %
- Addresses external access to the internal secure network	22.22	19.44	58.33	-	-
- Addresses encryption of data transit	-	-	-	-	-
- Addresses firmware and network security patching	-	-	-	-	-
- Utilizes secure protocols e.g. VPN, IPSEC	-	-	-	-	-
- Emphasizes segmentation of the network	-	-	-	-	-
- Prioritize most critical network assets	-	-	-	-	-

Table 4.5 indicates the knowledge technical staffs have on network security models available and in use in the institution networks, for the NSM 93.68% of respondents acknowledged the model excels at secure data transmission by use of encryption methods. Of the three security models respondents seemed most knowledgeable in the NSM and NASM with limited knowledge on the P2DR. In NASM; 73.68% of respondents' acknowledged network segmentation is addressed in the model, 55.26% acknowledge the model addresses prioritization of critical network assets and 55.26% of respondents agree utilization of secure protocol is addressed by the model, literature admits these as critical in securing network.

4.4 Challenges to network security Implementation

Table 4. 6: Factors affecting implementation of network security in universities

Factors affecting implementation of Network Security	**SD %**	**D %**	**N %**	**A %**	**SA %**
Unrestricted access of information within university	-	10.5	5.3	60.5	21.1
Legacy systems in the network	7.9	-	-	2.63	89.47
Decentralized network management	-	29.4	-	10.5	60.1
Decentralized decision-making regarding network security	-	43.2	12.5	-	44.3
Collaboration with other Institutions/Organizations	-	2.6	7.9	55.3	34.2
Highly technical and unpredictable student population	12.8	12.1	-	62.2	13.2
BYOD management in institution	22.2	42.8	7.8	12.2	15.0
BYOD is encouraged	15	29.4	-	35.3	20.3
Unpredictable network users	-	13.0		24.2	62.8
Local users threat to network security	-	33.9	12.6	30.7	22.8

Universities thrive on collaboration and exchange of scholarships and ideas both with people inside the university and outside the university and has its infrastructure built around these assumptions. Universities value the flow of information that is unrestricted, whether it's from collaboration

partners visiting lecturers or students. The third objective looked at factors that affect implementation of network security, 92.1 % of respondents acknowledging the existence of legacy systems operational on their institutional networks, which are a major security breach in network security as they have known vulnerabilities which attackers, capitalize on to gain access to the network.

A question was posed to respondents on decentralized network management where some sections, faculties or departments manage their own network segments including security, 70.6% acknowledged decentralized network management exists and is actually preferred with minimal over sight from management boards, with 44.3% of respondents acknowledging a decentralized approach of network management from university management boards was carried out by their institutions, as management boards leave responsibility of maintenance and security of networks to the respective sections, that request autonomy. 87% of respondents acknowledged their network users are unpredictable, with 53.5% of respondents acknowledging LAN users as a threat to network security this is not surprising due to the valued openness of information in universities and the dislike of constricted information flow preference, by usage of browser like tor that bypass security mechanisms or peer to peer file sharing applications that circumvent security.

Collaboration is a major aspect in university with its collaboration partners with 89.5 % of respondents acknowledging that collaboration partners have access to university networks.

4.5 Variables in the developed security model

Table 4. 7: P2DR variables implemented in securing university networks

	SD %	D %	N %	A %	SA %
Protection					
- Management provides support for network security.	22.22	33.33	25.0	19.45	
- Encryption of university data in transit and storage.	-	61.1	5.56	2.78	30.56
- Use of secure protocols in institutions	41.67	-	8.33	16.67	33.33
- Existence of network monitoring tools	60.53	5.26	5.26	7.89	21.06
- Firmware security patches carried out frequently	23.68	31.59	5.26	18.42	21.05
- Adequate skills level	13.16	44.74	-	23.68	18.42

- internet access regulated via proxy relays (BMO)	2.63	7.89	-	36.84	52.64
- Network Segmentation in the institution	-	49.39	15.67	22.73	12.21
- Existence of IPS on the network	10.44	66.07	8.39	12.30	2.80
Detection					
Real time active network monitoring	-	44.20	38.22	17.58	-
- Active event threat detection is carried out	13.89	58.33	5.50	22.28	-
- Active end point threat detection	8.3	16.7	-	-	75.0
- Existence of IDS on the network	23.68	28.95	10.53	36.84	-
- Network Threat Detection	47.37	31.58	-	13.16	7.89
-Active threat intelligence	21	63.2	-	15.8	-
-use of Security, Information, Event Management (SIEM)	-	31.6	50.0		18.4
Use of intruder traps e.g. honey pots	41.1	20.6	-	38.3	-
Response					
- Technical staff response to breach is satisfactory	26.32	13.16	10.52	50.00	-
- Actively hunting for threats based on past experiences	52.63	21.06	5.26	21.05	-
- ICT services crisis committee existence	-	78.94	5.27	15.79	-
-Communicate threat and counter measure to users (fewer than 10mins)	-	55.3	42.1	2.6	-
Recovery					
- Ability to contain damage and preserve assets	7.2	12.1	20.6	10.1	50.0
- Verification of affected assets	-	28.8	-	11.2	60
- Guidelines to restore business functions after breach	26.32	13.16	10.52	50.00	-
- Ability to close vulnerability	52.63	10.53	-	21.05	15.79
- clean up and restore services	-	12.79	5.27	78.94	-

Table 4.7 indicates the variables for the proposed network security model, **protection** is associated with reducing the attack surface, a mere 14.5% of respondents acknowledge that institutional management support network security, this is concerning as decentralized security management has been proven as a weak link in providing network security in organization (Li, 2017). Only 28.95% of respondents carry out any form of network monitoring, indicating most institution technical teams are unaware of patterns of network usage in their networks which can provide an indication of possible intrusion through unfamiliar traffic patterns, this in conjunction with the 15.1% of respondents who have implemented IPS on their institution networks is concerning with relation to network security, majority of institutions have no idea of who or what is using their networks and how. 55.37% of respondents acknowledge the lack adequate of skills to respond to network breaches that occur in their institutions, indicating there could be a problem in institution hiring practices or network security training is not a priority in the institutions. Though an impressive 89.48% of respondents utilize proxy relays on their networks masking the identity of the Local Area Network (LAN) users proving a layer of security.

The **detection** aspect of security noted active threat monitoring is barely carried out with 17.58% of respondents acknowledging real-time active network monitoring occurring in their institutions, 22.28% of respondents acknowledge active event threat detection is carried out in their institution and 18.4% of respondents acknowledge SIEM is utilized in their institutions, but an impressive 75% of respondents acknowledge end point monitoring exists in the institution indicating guidance is what is required for institutions to adopt better detection methods.

The **response** aspect of security with 50% of respondents acknowledge their response to network breaches is satisfactory, only 21.05% of respondents actively hunt for threats on institution networks indicating network security management is more reactive and not proactive. Of concern is merely15.79% of institutions have crisis committees in place to steer recovery process in the event of a catastrophic network breach occurs and an alarming 2.6% of respondents communicate to users of active threats and counter measures to those threats in institution networks.

The **recovery** aspect of security has 60.1% of respondents having the ability to contain network damage after an attack; interestingly 36.84% of respondents acknowledge the ability close vulnerabilities that would affect a network. An impressive 78.94% of respondents acknowledge the ability to clean up after a successful attack and restore services and 50% of respondents

acknowledge guidelines exist to restore business functions after a breach, indicating recovery measures are modestly implement in institutions

4.6 Correlation analysis

Table 4. 7: Spearman's correlation analysis matrix between variables

		PROTECTION	DETECTION	RESPONSE	RECOVERY	Secure_ Networks
PROTECTION	Correlation Coefficient	1.000	.923*	-.964	.908	.970
	Sig. (2-tailed)	.	.001	.004	.001	.004
	N	238	238	238	238	238
DETECTION	Correlation Coefficient	.923*	1.000	-.992	.898	-.992
	Sig. (2-tailed)	.001	.	.002	.003	.005
	N	238	238	238	238	238
RESPONSE	Correlation Coefficient	-.964	-.992	1.000	-.899	-.997
	Sig. (2-tailed)	.004	.002	.	.006	.002
	N	238	238	238	238	238
RECOVERY	Correlation Coefficient	.908	.898	-.899	1.000	-.978
	Sig. (2-tailed)	.001	.003	.006	.	.004
	N	238	238	238	238	238
Secure_Networks	Correlation Coefficient	.970	-.992	-.997	-.978	1.000
	Sig. (2-tailed)	.004	.005	.002	.004	.
	N	238	238	238	238	238

*. Correlation is significant at the 0.05 level (2-tailed).

A correlation analysis was used to determine the strength and direction of relationship between the variables, correlation coefficient range from -1.0 (perfect negative correlation) to + 1.0 (perfect positive correlation). To establish a correlation between secure networks, protection, detection, response and recovery spearman correlation rho was done.

The correlation matrix table (table 4.3) indicates the correlation between University Network Security and protection, detection, response and recovery. The correlations table also displays Spearman correlation coefficients, significance values (P-value) and the number of cases. A 2-tailed test significance value was chosen because the direction of association between these variables was

not known in advance. The significance level <0.05 indicates the correlation is significant and the two variables are linearly correlated. A variable correlated to its self gives a coefficient of 1 as shown in the matrix.

The variables **protection, detection, response and recovery** have strong correlation to each other the correlation between protection and detection is at .923** the two variables have a strong positive correlation relationship, with a significant value of 0.01 indicating a statistically significant bivariate association between the two variables. Protection and recovery is at .908 indicating a positive correlation relationship between protection and recovery variable this indicates a statistically significant bivariate association between the two variables with a strong significant level of 0.01.

Protection and response are significantly and strongly positively correlated r = -.964, N= 238, p = 0.004.

It is also indicated that the correlation coefficient for network security and protection is .970with a P-value of 0.04 from the 238 respondents. This also shows there is a strong positive linear relationship between network security and protection. Since the P-value is 0.04 which is less than 0.05, the null hypothesis is rejected and the conclusion is there is a significant positive linear relationship between protection and network security. The correlation coefficient between response and network security is -.997 with a P-value of 0.02 from the 238 respondents. Since the P-value is less than 0.05, the null hypothesis is rejected and it is concluded that there is a significant negative linear relationship between the implementation of response and network security. The correlation coefficient between detection and network security is -.992 with a P-value of 0.05 a perfect significance between the two variables from the 238 respondents.

The correlation between network security and recovery is -.978 with a significance value of .004 since the P-value is less than 0.05, the null hypothesis is rejected and it is concluded that there is a significant negative linear relationship between the implementation of recovery and network security.

4.7 Logistic Regression analysis

Logistic regression is used because the researcher wanted to predict the categorical dependent variable from the analysis. The analysis is used to determine that the data generates a secure (+1) or insecure (-1) outcome, exponentiation of the beta values is used to change the results into an odds ratio (OR). The OR represents the odds of an outcome occurring given a particular event, compared

to the odds of the outcome occurring in the absence of that event if the OR is greater than 1, then the event is associated with a higher odd of generating a positive outcome occuring. Conversely, if the OR is less than 1, then the event is associated with a lower odd of that outcome occurring (Press & Wilson, 1978).

Logistic regression provides a coefficient "expB" which measures each independent variable's partial contribution to variations in the dependent variable. Secure network is the dependent variable, with dichotomous responses (i.e secure or insecure). The independent variables are protection, detection, response and recovery which are all categorical variables, there were no extreme points or outliers in the data, the dependent variable is dichotomous.

Z-scores or standardized scores are used in the study. In the study, we have responses from technical staff regarding protection, detection, response and recovery. How are they compared? The answer is Z-scores. Z-scores are standardized deviations from the mean. The purpose of Z-scores is to identify and describe the exact location of every score in a distribution (Salkind & Rainwater, 2006) Standardizing scores facilitate the interpretation of a single test score. In this case, the z-scores are used to run a binary logistic regression analysis to indicate the strength of each security mechanism with regards to secure university network. To predict the outcome of secure university networks, a mathematical model or logit function was created that included all predictor variables that were useful in predicting the dependent variable.

Table 4. 8: Variables in the Equation

		B	Df	Sig.	Exp(B)
Step 1[a]	PROTECTION	1.859	1	.001	6.420
	DETECTION	-2.102	1	.000	.122
	RESPONSE	-.569	1	.001	.566
	RECOVERY	-.851	1	.002	.427
	Constant	4.619	1	.000	.354

Table 4.9 gives all variables, the Sig column, the p-values are all below 0.05 (alpha). Protection with a significant value of 0.001, detection has a significant value of 0.000, response has a significant value of 0.001 and recovery has a significant value of 0.002 this means that the regression test for Secure Networks and protection, detection, response and recovery are significant and have strong relationship once the other variables are controlled for, there is a strong enough relationship between each of the variables to secure university networks. To interpret the

differences between effects of respective secure network to the predicted variable, the exp (B) column which represents the odd ratios for the individual variables is used. It should be noted that;

Probability (p)= odd ratio/1+odd ratio……eqn (1)

Protection is 6.420 times more likely to secure university networks, detection is 0.122times more likely to secure networks, response is 0.566 more times likely to secure networks while recovery is 0.4.27 more likely to secure university network. This table generally gives the magnitude of the effects of the predictor variables are have on the outcome of the dependent variable. In the model, the B values for each variable are also considered. The co-efficients for the model are contained in the column headed B.

The full model (logit function) being tested is as follows;

$Y = \beta 0 + \beta 1_{x1} + \beta 2_{x2} + \beta 3_{x3} \ldots\ldots\ldots\ldots\ldots\ldots\ldots eqn$ (2)

$Y = 4.619 + 1.859_{x1} + -2.102_{x2} + -.569_{x3} + -.851_{x4}$

Y= 2.956

Where;

Y is the probability of secure networks

x1= Protection

x2= Detection

x3=Response

x4= Recovery

The figure 4.1 below represents a graphical representation of the network security model developed from the data analysis, where if the sig (p) value is < 0.05, the X_* variable is valid in determining the Y variable and the probability of Y being secure or insecure, with p=1 representing secure or q-p= 0 representing insecure. The model satisfies eqn 1.

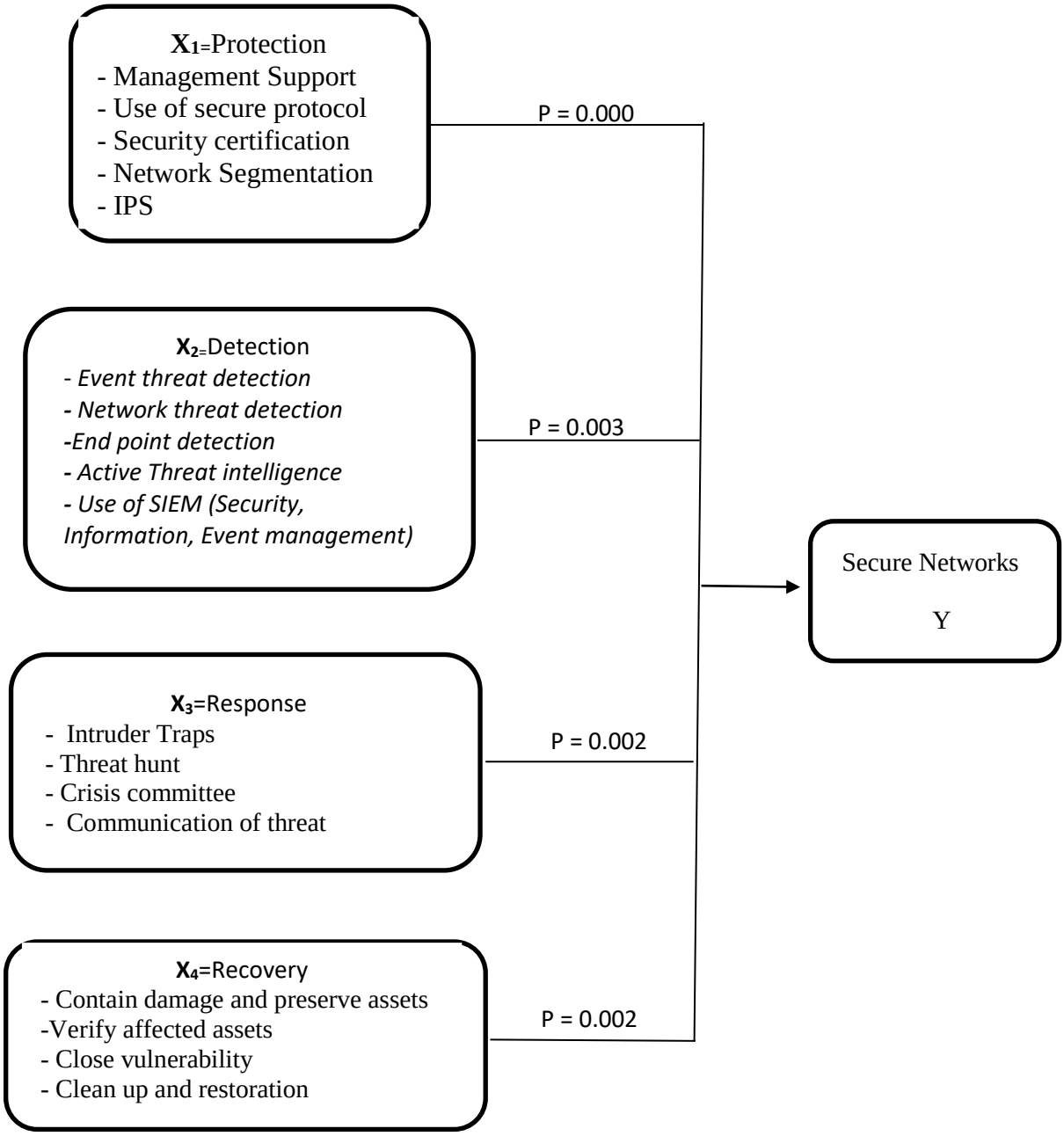


Figure 4. 1: Developed network security model with active detection security component

Table 4. 9: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.799[a]	0.638	.608	0.33412

a. Predictors: (Constant), RECOVERY, DETECTION, RESPONSE, PROTECTION

The R value represents the correlation between the dependent and independent variable, a value greater than 0.4 is taken for further analysis, in this case, the value is 0.799, which is good.

In terms of variability, the value R^2=0.638 or 64% explains the total variation for the dependent variable that could be explained by the independent variables, a value greater than 0.5 shows the model is effective enough to determine the relationship, in this case the value of 0.638 is good. The adjusted R^2gives a revised generalized estimate of the results, it is required to have a difference between R-square and Adjusted R-square minimum, in this case indicating 0.608 which is not far from 0.638, so it is good.

Table 4. 10: Anova

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	97.585	4	24.396	66.720	.001[b]
	Residual	94.215	240	.230		
	Total	192.800	244			

a. Dependent Variable: Secure Networks

b. Predictors: (Constant), RECOVERY, DETECTION, RESPONSE, PROTECTION

Generally, 95% confidence or a significant level of 5% of the study was chosen, the p-value should be less than 0.05 and the value of the study on the table is 0.01. Therefore, the result is significant. The F ratio represents the improvement in the prediction of the variable by fitting the model after considering the inaccuracy present in the model. A value greater than 1 for F-ratio yield an efficient model, table 4.11 provides a value of 66.720, which is good.

CHAPTER FIVE
SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter gives a summary of the research conducted, conclusions based on the results and recommends further research that should be done to enhance information security on university network infrastructure.

5.2 Summary

The main purpose of this study was to come up with a network security model for use on university data networks to protect from unauthorized access and ensure network breaches are managed effectively.

The study got responses from 238 respondents who included technical staff involved with the installation, maintenance and management personnel of university network infrastructure, the study was conducted in Kenya and covers chartered universities in the country. Protection, detection, response and recovery mechanisms implemented at the institutions were collected. Quantitative data was collected using structured questionnaires. The data was then coded and analyzed using SPSS version 25. The results of the analysis were used to form a network security model to secure university networks.

5.3 Discussions

5.3.1 Network Models used in securing universities.

Appendix 3 identifies network models widely used on the internet and in university networks have had glaring weaknesses since their inception and relied on internet Request for Comments (RFC) to correct specific issues identified by users, of the two network models the OSI model and TCP/IP model, with the latter noted being the most used in Kenyan university networks at 72.2% evidenced by Table 4.3. Network Security Model SWOT analysis carried out by various research authors identified NSM as ideal for point to point connection over a hostile network environment that utilizes a third party organization that manages the network traffic between the two points, usage of public and private keys is also utilized, it was noted the overheads in transmission, encryption and

sharing of security keys were too high for use on a LAN. The NASM on the hand was ideal and catered for most of the weaknesses of the network models, with a flaw of not considering monitoring aspect of networks. The P2DR network was not specifically designed for data communication networks but had been used in automation industries to manage SCADA communication, plus it was designed as a malleable model, which users can customize to respective industries, plus its biggest strength is emphasis on monitoring.

5.3.2 Network models and Network Security models.

To establish the effectiveness to network security models, secondary data on SWOT analysis was collected, Appendix 3. Analysis of Privacy Preserving Demand Response (P2DR) Model representing the network security models; it was noted the TCP/IP and OSI network models tend to compete with each other on usage within Kenyan university networks. Kenyan universities were noted to having a preference for the TCP/IP model, refer to Table 4.7, these network models have weaknesses inherent to them. The OSI for example was not to be theoretical and does not provide clarification for network development and has duplication of services e.g transport and data link both have error control mechanisms, their also exists interdependence among layers, the OSI layers cannot work in parallel to each other, they work once data is received from the predecessor layer. TCP/IP model addresses these issues by merging layers that have duplication of services and its scalable which provides clarification for network development allowing cross platform communication among heterogeneous networks. As much as it addresses flaws in its predecessor it also has flaws that network security models try to address. The NSM addresses one aspect of network security which point to point encrypted network transmission over TCP/IP networks; the NASM goes a step further to address security based on physical attributes of networking infrastructure, the virtual networking attributes of the networking systems, allowing and deny access between network hosts and other networks, patching candence is addressed by the model, training of end user clients on network hygiene and training of administrative and management staff, the model however lacks monitoring aspect of network that would make technical users proactive to threats, The P2DR model weakness is its biggest strength for the study, the fact that it is not industry specific makes it malleable, where strengths of the NSM and NASM were incorporated with the strengths of the P2DR as functions of security, that designed and were analyzed to come up with the proposed model.

5.3.3 Barriers in implementation of secure networks.

The valued openness and free access to information is evident as 89.5% of respondents acknowledge collaboration with other institutions and organizations exist this poses a problem when trying to secure university networks especially when collaboration partners require unfettered access to the institutional network. A question posed to respondents on the existence of unrestricted flow of information on institution networks, 81.6% of respondents acknowledged this to be true, once a user has access to the institution networks no restriction exist on what can be accessed and from where, this coupled with 92.1% of respondents acknowledging existence legacy systems older than 10 years is a major security threat on institutional networks, essentially a rogue user who is unmonitored and unmanaged would capitalize on known vulnerabilities of the legacy systems causing catastrophic failures on the network, evidenced by Pen state, school of Engineering network breach (Cenzic, 2014). 70.6% of respondents acknowledged institutions ran decentralized network management, where autonomous sections of the university network existed and were managed independent of ICT departments, this leads a reactionary type of security set up, as all entry points of the institution network will not be monitored, this would create a security lapse in securing university networks. 55.6% of respondents acknowledged BYOD is encouraged in their institution, of concern is only 27.2% of institutions manage BYOD in their institution. This is especially of concern as 75.4 % of respondents acknowledge they consider their network users unpredictable while 53.5% of respondents consider local network users as threats to institutional networks, this coupled with unmanaged BYOD pose serious security threat on institutional networks. BYOD devices are known to create a large attack surface to university networks, due to poor patching by users and malware infected systems by the time they join institutional networks evidenced by (Olalere et al., 2015).

5.3.4 Suggested security components to be integrated to create secure university networks.

Prior to suggesting which information security measure be implemented to control and ensure secure university networks, consideration was done in respect to the existing network security threats and vulnerabilities. The measures of protection, detection, response and recovery that had been deployed in the institution networks were analyzed to gauge their effectiveness. Respondents

were tasked on giving details on how institutional networks were secured in relation to protection, detection, response and recovery. In regard to protection 33.34% of respondents of university data being intentionally encrypted before transmission and during storage, 50% of respondents acknowledged the use of secure protocols e.g. IPSEC in management of the networks, 28.95% of respondents acknowledge usage of network monitoring tools in the institutions with 39.47% of respondents agreeing candence patching is carried out in the organization. 34.94% of respondents agreed network segmentation is carried in the institution and 89.48% of responds acknowledged proxy relays are used on the intuition, from the data it's evident that protection measures are implemented but need better implementation.

For the detection measures the study tried to find out if institutions utilize active network monitoring techniques to enable a proactive defense system, it was noted only 17.58% of respondents carry out active monitoring on their networks, 22.28 of respondents utilize active event threat detection, 15.8% utilize active threat intelligence, 18.4% of respondents utilize of Security Information Event Management (SIEM) systems, with 38.3% of respondents acknowledge use of intruder traps but, an impressive 75% utilize active end point detection on institutional networks. What is evident from the data is institutional networks are set up to be reactive to network breaches but not proactive, only end point systems on the network are monitored for active threats.

For the response measures what stood out was the week communication on network beaches with only 2.6% of respondents acknowledging after a network breach occurs, the attack is communicated and counter measures to counter the breach are communicated as well. Of concern was institutions barely have crisis steering committees in the institutions to manage breaches and recovery process with 15.79% of respondents acknowledge crisis steering committees exist in the institutions.

For the recovery measure an impressive 71.2% of respondents are confident enough to verify which network assets have been breached with 60.1% of respondents having the confidence to contain the damage associated with a breach and 78.94% confident enough to clean after breach and restore service back to normal operations, the data indicates recovery of the network after is not a problem. Institutions seem to struggle with active detection of network threats and response in the event of a breach.

5.4 Conclusions

The study analyzed OSI and TCP/IP models, these models were noted to ensure interoperability between devices from different vendors and also enable connection and connectionless oriented services which are critical in the information technology world because it breaks barriers that may be association with data communication, their major flaw is their theoretical and do not provide satisfactory clarification of security in data communication, these models are best used as benchmark in deployment and implementation of networks for optimum data communication. Analysis of the network security models revealed the NSM is best suited for securing data communication over Wide Ares Network (WAN) architectures with high transmission overheads of third party security partners, secure exchange of keys, encryption and decryption. The NASM capitalizes and addresses on weaknesses of the OSI and TCP/IP models by merging duplicated services and introducing the security aspect to the model. It addresses the NSM weaknesses by stripping of the financial and computing overheads and introduction of security measures for use on Local Area Networks (LAN) but is limited in aspects of network monitoring. The P2DR model is malleable so it is used to custom build an adequate network security model by capitalizing on the strengths of existing network and network security models and introducing the aspect of active monitoring within its layers.

Analysis of factors affecting implementation of network security in universities noted the existence of very a large population with a variety of BYOD that are used to gain access to the institutions networks, that with highly unpredictable behavior when using the network, keen on bypassing security measures with desires of unrestricted access to information whether for consumption or collaboration.

The study introduces the network security model on Figure 4.2 which addresses the broad nature of the network security models in the study, it addresses the weaknesses of existing network and security models of complexity, duplication of services, specific to certain network topologies and lack of monitoring. It provides clarification for practical security implementation by describing the steps to follow to secure a network. The model can be used as a template in securing institutional networks, by utilizing active network monitoring. In the future the researcher hopes the model created would reduce unauthorized network access in Kenyan universities.

5.5 Recommendations

Training of staff on network security helps technical staff to have confidence in the network they are administering, this is key in correctly implementing network security models and avoids

technical staff from interpreting the models individualistically, so that the technical staff can be aware of the strengths, weakness and threats inherent within particular network or network security models.

The study noted a structured security system is required for universities to have clients access the network, without infringing on the openness they value so much, an onion ring layer security approach could be implemented in universities, with security parameters getting more intense the closer to the core, with the most security sensitive clients and data nearer to the core of the security rings and less critical systems and information on the outer rings.

Regular network audits ensure that loopholes in network systems are detected and any network configuration inconsistencies can also be addressed. Audit trails need to be done frequently to control flaws that would become threats. Proper training is adequate for network security as threat actors adapt to existing security parameters implemented and create mechanisms to easily bypass existing security measures, training ensures that the technical staff are competent on security mechanisms implemented, that are compromised or maybe compromised and how to deal with those compromises, including evolving best practices of security configurations and implementations. Frequent maintenance is required in any organization. Monthly maintenance is recommended to be one of the best ways of managing university network infrastructure, maintenance involves corrective, adaptive and preventive.

5.6 Suggestions for further research

The researcher noticed security certifications and trainings were not of priority in Kenyan universities, this could be a lapse in employment practices or lack of budget allocation, the study noted institutional technical personnel were willing to tackle network threats but admitted to lacking the skills to address the ever evolving threats, a study needs to be conducted to address this shortcoming in security policy.

Research also needs to be done to understand the institutions administrative aspect in network security; the study reveals information security policies are set in place as a formality but implementation is very poor. Aspects of information security implementations seem to be left to the discretion of the technical staff.

REFERENCES:

ACSC.(2017). *Cybersecurity Threats and Responses in the Australian Higher Education Sector* [NAtional Cyber Security Status].Australian Cyber Security Centre.https://www.cyber.gov.au/newsletter/issue-36/cybersecurity-threats-and-responses-in-higher-education-sector [Accessed 16 Feb. 2020].

Abdulghani, S. (2009). Design and Implementation of a Network Security Model for Cooperative Network. *International Arab Journal of E-Technology*, *1*, 26–36.

Aguilar-Saven, R. S. (2004). Business process modelling: Review and framework. *International Journal of production economics*, *90*(2), 129-149

Ahmad, H., Francis, A., &Zairi, M. (2007). Business Process Reengineering:critical success factos in higher education. *Bussiness Process MAnagement*, *J*(13), 451–469. https://doi.org/10.1108/1463710710752344 [Accessed 16 Jan. 2020].

Aineah, A. (2019). *Student hackers: Exposing varsities' vulnerable systems*. Standard Entertainment and Lifestyle.https://www.standardmedia.co.ke/entertainment/local-news/2001268941/student-hackers-exposing-varsities-vulnerable-systems [Accessed 16 Mar. 2020].

Alesini, D., Bertolucci, S., Bellaveglia, M., M.E.Biagini, R.Boni, Boscolo, M., Castellano, M., Clozza, A., Di Pirro, G., Drago, A., Esposito, A., Ferrario, M., Filippetto, D., Fusco, V., Alessandro, G., Ghigo, A., S.Guiducci, Incurvati, M., Ligi, C., & Emma, P. (2004).*THE SPARX PROJECT: R&D ACTIVITY TOWARDS X-RAYS FEL SOURCES* AND DISASTER RECOVERY http://www.JACoW.org [Accessed 14 Feb. 2021].

Alharbi, T., &Tassaddiq, A. (2021).*Assessment of Network Security Awareness among students of Majmaah University*.*5*(23), 1–15. https://doi.org/10.3390/bdcc5020023 [Accessed 18 Feb. 2021]

Almaiah, M. A., Al-Khasawneh, A., & Althunibat, A. (2020). Exploring the critical challenges and factors influencing the E-learning system usage during COVID-19 pandemic. *Education and Information Technologies*, 1–20. https://doi.org/10.1007/s10639-020-10219-y [Accessed 18 Mar. 2021]

Al-Safwani, N., Fazea, Y., & Ibrahim, H. (2018). ISCP: In-depth model for selecting critical security controls. *Computers & Security*, *77*, 565–577.

Aluvala, S., Sekhar, K. R., &Vodnala, D. (2016). An Empirical Study of Routing Attacks in Mobile Ad-hoc Networks. *Procedia Computer Science*, *92*, 554–561. https://doi.org/10.1016/j.procs.2016.07.382 [Accessed 8 Jan. 2021]

Appel, S., Kleber, P., Freudenreich, T., &Buchmann, A. (2014).*Modeling and execution of event stream processing in business processes. Information Systems* (46th ed.).

Aron Antony Charles, M., & Sasikumar, N. (2018). Impact of Concept Mapping and Modular Learning Techniques on Pupils' Achievement for the Selected Topics in Mathematics. *American Journal of Educational Research*, *6*(6), 649–657. https://doi.org/10.12691/education-6-6-11

Asiko, E. (2019). *Effects of business process re-engineering on public sector service delivery in Kenya: A case study of Kenya Universities* [Doctoral thesis, Africa Nazarine University]. http://repository.anu.ac.ke/bitstream/handle/123456789/515/Elizabeth%20Asiko.pdf?sequence=1 [Accessed 18 Mar. 2021]

AT&T, B. L. (2015). Security Problems in the TCP/IP Protocol Suite.*Computer Communication Review*, *19*(2), 32–48. https://www.cs.columbia.edu/~smb/papers/ipext.pdf [Accessed 19 Mar. 2021]

Barnard, L., & Von Solms, R. (2000). A formalized approach to the effective selection and evaluation of information security controls. *Computers & Security*, *19*(2), 185–194.

Barlette, Y., Jaouen, A., & Baillette, P. (2021). Bring Your Own Device (BYOD) as reversed IT adoption: Insights into managers' coping strategies. *International Journal of Information Management*, *56*, 102212. https://doi.org/10.1016/j.ijinfomgt.2020.102212 [Accessed 18 Feb. 2021]

BBC. (2019, June 15). Top universities under "ransomware" cyber-attack.*BBCNews*.https://www.bbc.com/news/education-40288548 [Accessed 2 Mar. 2021]

Bechkoum, K. (2020, July 18). *Cyber-threats increasing for universities under lockdown* [Educational]. University World News, The Global Window on Higher Education. https://www.universityworldnews.com/post.php?story=20200717134543848 [Accessed 20 Mar. 2021]

Bennett, P. Y., Rosemary. (2017, September 5). University secrets are stolen by cybergangs. *The Times*.https://www.thetimes.co.uk/article/university-secrets-are-stolen-by-cybergangs-oxford-warwick-and-university-college-london-r0zsmf56z [Accessed 21 Mar. 2021]

Bhise, A., &Kamble, S. (2016). Detection and Mitigation of Sybil Attack in Peer-to-peer Network.*International Journal of Computer Network and Information Security*, *8*, 56–63. https://doi.org/10.5815/ijcnis.2016.09.08

Blackfield, J., & Bambernek, J. (2021). *Network Access Security Model* (pp. 1–32) [Network Security]. SANS. https://sansorg.egnyte.com/dl/UuJKXotLWA/?

Bongiovanni, I. (2019). The least secure places in the universe?A systematic literature review on information security management in higher education.*Computers& Security*, *86*, 350–357. https://doi.org/10.1016/j.cose.2019.07.003

Brewster, T. (2012, August 30). *Oxford University Beefs Up Security After "Anonymous" Threat | TechWeekEurope UK*. Silicon UK.https://www.silicon.co.uk/workspace/oxford-university-security-anonymous-hack-90815 [Accessed 2 Apr. 2021]

Brittin, E. G., Tavs, J., & Bournas, R. (1995). TCP/IP: The next generation. *IBM Systems Journal, Volume: 34*(Issue: 3), 452–471. https://doi.org/10.1147/sj.343.0452

Broadhurst, R., & Chang, L. (2016). Cybercrime in Asia: Trends and Challenges. In *Handbook of Asian Criminology* (pp. 49–63).https://doi.org/10.2139/ssrn.2118322

Business Today. (2015, October 28). *Cost of cyber-crime hits Ksh15bn, new report says—Business Today Kenya*. https://businesstoday.co.ke/cost-of-cyber-crime-hits-ksh15bn-new-report-says/ [Accessed 20 Dec. 2020]

CAK. (2019, December 5). *Cyber-Attacks On The Rise In Kenya*. Communications Authority of Kenya.https://ca.go.ke/cyber-attacks-on-the-rise-in-kenya/ [Accessed 20 Dec. 2020]

Cenzic. (2014, February 25). *Cenzic Announces New Application Security Service For The Connected Enterprise* [Information Week IT Network]. Dark Reading.https://www.darkreading.com/applications/cenzic-announces-new-application-securit/240166273 [Accessed 22 Dec. 2020]

Chapman, J. (2019). *How Safe is Your Data?: Cyber-security in Higher Education*. Higher Education Policy Institute.

Chapman, C. (2016). Chapter 3 - Locking down the infrastructure: Internet, Wi-Fi, wired, VPN, WAN, and the core. In C. Chapman (Ed.), *Network Performance and Security* (pp. 39–83). Syngress. https://doi.org/10.1016/B978-0-12-803584-9.00003-2

Charter, R. A. (1999). Sample size requirements for precise estimates of reliability, generalizability, and validity coefficients. *Journal of Clinical and Experimental Neuropsychology*, *21*(4), 559–566.

Chen, Y., & He, W. (2018). Security risks and protection in online learning.*ASurvey.Int.Rev. Res. Open Distrib. Learn*, *14*, 108–127. http://www.irrodl.org/index.php/irrodl/article/view/1632

Chesbrough, H., &Rosenbloom, R., S. (2002). The role of the business model in capturing value from innovation: evidence from Xerox Corporation's technology spin-off companies. *Oxford Journals, 11*(3), 529–555.

Coleman, V. (2015, April 28). *Cyber-attack causes Rutgers internet service interruptions*. Nj. https://www.nj.com/middlesex/2015/04/cyber_attack_against_rutgers_causes_internet_servi.html [Accessed 18 Dec. 2020]

Collins, M. W., & Morris, S. B. (2008). Testing for adverse impact when sample size is small. *Journal of Applied Psychology*, *93*(2), 463.

Costa, L. (1998). Open Systems Interconnect (OSI) Model. *JALA: Journal of the Association for Laboratory Automation, 3*(1), 28–35. https://doi.org/10.1177/221106829800300108

Coughlan, S. (2020, September 17). Cyber threat to disrupt start of university term.*BBCNews*.https://www.bbc.com/news/education-54182398 [Accessed 2 Jan. 2021]

Creswell, J. W. (2002). *Educational research: Planning, conducting, and evaluating quantitative*. Prentice Hall Upper Saddle River, NJ.

CSIS.(2017). *Global Cyber Strategies Index | Center for Strategic and International Studies* [Information Security]. Center for Strategic &Interna. https://www.csis.org/programs/strategic-technologies-program/cybersecurity-and-governance/global-cyber-strategies-index [Accessed 28 Dec. 2020]

CSIS.(2021). *Significant Cyber Incidents | Center for Strategic and International Studies* [Strategic Technologies].Significant Cyber Incidents.https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents [Accessed 22 Dec. 2020]

Cuchta, T., Blackwood, B., Devine, T. , Daniels, K. ., Lutjens, C., H., Maibach, S., & Stephenson, R. .(2019). Human Risk Factors in Cybersecurity.*20th Annual SIG Conference on Information Technology Education*, 87–92.

Commision for University Education. (2020). *Commission for University Education—Accreditation* [GoK Informational]. Https://Imis.Cue.or.Ke/RecognitionAndEquationforQualifications/AccreditedUniversities. https://www.cue.or.ke/index.php?option=com_content&view=category&layout=blog&id=13&Itemid=471 [Accessed 29 Dec. 2020]

Cui, Y., Qian, Q., Shen, G., Guo, C., & Li, S. (2020). REVERT: A Network Failure Recovery Method for Data Center Networks. *Electronics*, *9*(8), 1187. https://doi.org/10.3390/electronics9081187

Custer, W., L. (2010). Information security issues in higher education and institutional research. *2010 Wiley Periodicals, Inc*, 23–49.

Clatot, J.-P. (2017, September 5). UK universities targeted by cyber-thieves. *BBC News*. https://www.bbc.com/news/technology-41160385 [Accessed 20 Feb. 2021]

Danesh, A. (2021). *SWOT Analysis for Open Systems Interconnection (OSI) Reference Model*. https://doi.org/10.13140/RG.2.2.35340.95368

Daily Monitor.(2005). *Why cybercrime is rising in Ugandan Universities* [Daily Newspaper Digital print].Daily Monitor.https://www.monitor.co.ug/uganda/education/prosper/why-cyber-crime-is-rising-1831128 [Accessed 22 Dec. 2020]

Daya, B. (n.d.). *Network Security: Histrory, Importance and Future* (pp. 1–13) [Network Security]. University of Florida; Department of Electrical and Computer Engineering.https://www.aimt.edu.in/wp-content/uploads/2016/12/Network-Security.pdf [Accessed 20 Mar. 2020]

De Vellis, R. F. (2003). Scale Development: Theory and Applications (2nd ed., Vol. 26). Thousand Oaks, CA: Sage Publications.

Dey, M. (2011). Business Continuity Planning (BCP) methodology—Essential for every business.*2011 IEEE GCC Conference and Exhibition (GCC)*, 229–232.https://doi.org/10.1109/IEEEGCC.2011.5752503

DIaz, A., Sherman, A., & Joshi, A. (2018).*A Study of User Susceptibility and Behavior*.*arXiv 2018*.https://doi.org/1811

Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. *Computers & Security*, *92*, 101747. https://doi.org/10.1016/j.cose.2020.101747

District of New Jersey, U. S. A. (2018, October 26). *Computer Hacker Who Launched Attacks On Rutgers University Ordered To Pay $8.6m Restitution; Sentenced To Six Months Home Incarceration* [United States Department of Justice]. United States Attorney's Office: District of New Jersey. https://www.justice.gov/usao-nj/pr/computer-hacker-who-launched-attacks-rutgers-university-ordered-pay-86m-restitution [Accessed 6 Jun. 2019]

EDGUARDS. (2018, June 15). *Higher Education Cyber Attacks History*.EdGuards - Security for Education.https://edguards.com/pr/articles/higher-education-cyber-attacks-history/ [Accessed 20 Jun. 2019]

educause. (2021). *Business Continuity and Disaster Recovery* (Higher Education, Vol. 10).https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/business-continuity-and-disaster-recovery [Accessed 16 Jul. 2019]

FireEye, I. (2015). *Why Cyber Attackers Are Targeting Higher Education, and What Universities Can Do about It.*Libary catalog. www.fireeye.com

Forza, C. (2002). Survey research in operations management: A process based perspective. *International Journal of Operations & Production Management*, *22*(2), 152–194. https://doi.org/10.1108/01443570210414310

Forouzan, B. A. (2002). *TCP/IP protocol suite*. McGraw-Hill Higher Education.

Gil-Jaurena, I. (2013). Openness in higher education.*Open Praxis*, *5*(1), 3–5.

Golafshani, N. (2015). Understanding Reliability and Validity in Qualitative Research. *The Qualitative Report*. https://doi.org/10.46743/2160-3715/2003.1870

Hunt, G. (2002). *TCP/IP Network Administration, 3rd Edition [Book]*. O'Reilly Media, Inc. https://www.oreilly.com/library/view/tcpip-network-administration/0596002971/

Hatton, C. (2017, May 15). Ransomware cyber-attack: Who has been hardest hit? *BBC News*. https://www.bbc.com/news/world-39919249 [Accessed 10 Aug. 2019]

Harris, C. E., &Hammargren, L. R. (2016). Higher education's vulnerability to cyber-attacks. *University Business*, *8*, 16.

Hartpence, B. (2013). 1. Networking Models - Packet Guide to Core Network Protocols [Book]. In *O'reilly* (pp. 80–85). O'reilly. https://www.oreilly.com/library/view/packet-guide-to/9781449308094/ch01.html [Accessed 16 Jul. 2019]

Höne, K., &Eloff, J. H. P. (2002). Information security policy—what do international information security standards say? *Computers & Security*, *21*(5), 402–409.

Hubaux, J.-P., Buttyan, L., &CapkunI, S. (2001). The Quest for Security in Mobile Ad Hoc Networks.*MobiHOC*, 1–10.

Jang-Jaccard, J., & Nepal, S. (2018). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

Johnson, J. (2021, January 25). *Industries most targeted by malware 2019* [Statistical Data Analysis]. Statista.https://www.statista.com/statistics/223517/malware-infection-weekly-industries/ [Accessed 10 Jun. 2020]

Jorrigala, V. (2017).*Business Continuity and Disaster Recovery Plan for Information Security*. 90. https://repository.stcloudstate.edu/cgi/viewcontent.cgi?article=1068&context=msia_etds [Accessed 26 Jun. 2019]

Kajilwa , G. (2016, July 18). Attackers Demand Sh700,000 Ransom from Nairobi University. STANDARD Digital. Retrieved September 9, 2016, from http://www.standardmedia.co.ke/article/2000208977/university-of-nairobi-s-cyber-attack-contained-says-ca/?pageNo=1 [Accessed 27 Jun. 2020]

Kaimba, B., Abuli, M., Munyendo, B., Ndungu, M., Wanjohi, M., Rishad, N., Muchiri, B., Kamau, D., &Adhiambo, J. (2020).*Local Perspective on Data Protecyion and Privacy Laws* (Serianu; Africa Cyber Report 2019/2020: Kenya, pp. 1–104)

Kalniņš, R., Puriņš, J., &Alksnis, G. (2017).Security Evaluation of Wireless Network Access Points.*Applied Computer Systems*, *21*(1), 38–45.https://doi.org/10.1515/acss-2017-0005

Kelly, S. E., Bourgeault, I., & Dingwall, R. (2010). Qualitative interviewing techniques and styles. *The SAGE Handbook of Qualitative Methods in Health Research*, 307–326.

KERR, J. A. (2018). EBSCOhost | 139171629 | Information, Security, and Authoritarian Stability: *International Journal of Communication*, *12*((19328036)), p3814-3834. https://doi.org/21p

kenya cyber security report. (2019, July 10). *Kenya cyber security report 2019* [Cyber Security]. EAST AFRICA RECOVERY EXPERTS. https://eastafricarecoveryexperts.com/tag/kenya-cyber-security-report-2019/ [Accessed 16 Dec. 2019]

Khan, M. (2017). COMPUTER SECURITY IN THE HUMAN LIFE. *International Journal of Computer Science and Engineering (IJCSE)*, *6*, 35–42.

Kimani, K., Muchai, C., MWangi, M., Shiyayo, B., Kisutsa, C., &Kigen, P. (2014).*SERIANU: Kenya Cyber Report 2014* (Annual 3th Edition; Rethinking Cyber Security – "An Integrated Approach: Processes, Intelligence and Monitoring.," p. 44).Serianu Limited. https://www.serianu.com/downloads/KenyaCyberSecurityReport2014.pdf

Klovig Skelton, S. (2018, September 11). *Higher education sector's poor response to cyber threats laid bare in EfficientIP report*. ComputerWeekly.Com. https://www.computerweekly.com/news/252448482/Higher-education-sectors-poor-response-to-cyber-threats-laid-bare-in-EfficientIP-report [Accessed 16 Jun. 2019]

Kothari, C. R. (2004). *Research methodology: Methods and techniques*. New Age International.

Kullgren, J. (2019). *Challenges and advantages brought by P2DR, PDS2: interview with EVRY*. https://thepaypers.com/interviews/challenges-and-advantages-brought-by-pds2-interview-with-evry--1239759

Kumar, G., & Kumar, K. (2014).Network security – an updated perspective. *Systems Science & Control Engineering*, *2*(1), 325–334. https://doi.org/10.1080/21642583.2014.895969

Kumar, M. (2012, January 18). *100 Kenya government websites breached by Indonesian hacker*. The Hacker News.https://thehackernews.com/2012/01/100-kenya-government-websites-breached.html [Accessed 24 Jun. 2020]

Kumar, R., &Dhanda, N. (2017).An Evaluation of OSI Reference model and comparison with TCP/IP Model.*International Journal of Engineering and Techniques*, *3*(4), 1–4.

Lawshe, C. H. (1975). A quantitative approach to content validity. *Personnel Psychology*, *28*(4), 563–575.

Lee, J. (2020, October 30). *Security Threats Facing Universities* [Information Security].Infosecurity Magazine.https://www.infosecurity-magazine.com:443/opinions/security-threats-universities/ [Accessed 6 Jun. 2021]

Lennon, M. (2010, April 20). *Symantec unveils Global Internet Security Threat Report for 2009 | SecurityWeek.Com* [Information Security Status Report]. Security Week.https://www.securityweek.com/content/symantec-unveils-global-internet-security-threat-report-2009 [Accessed 16 Dec. 2020]

Lessing, M. (2020).*Case Study: WannaCryRansomware* [Information Security]. SDxCentral.https://www.sdxcentral.com/security/definitions/case-study-wannacry-ransomware/[Accessed 6 Jun. 2019]

Lewis, J. (2011). *Time Line of Major Global Cyber Incidents 2010-2011* [Information Security].Bank Info Security.https://www.bankinfosecurity.com/time-line-major-global-cyber-incidents-2010-2011-a-3440 [Accessed 16 Oct. 2020]

Li, T. (2017). Analysis on the University's Network Security Level System in the Big Data Era. *IOP Conference Series: Earth and Environmental Science*, *100*, 012031. https://doi.org/10.1088/1755-1315/100/1/012031

Li, T. (2017). Analysis on the University's Network Security Level System in the Big Data Era. *IOP Conference Series: Earth and Environmental Science*, *100*, 012031. https://doi.org/10.1088/1755-1315/100/1/012031

Liu, C., W., Huang, P., & Lucas, H. (2019). Centralized IT Decision Making and Cybersecurity Breaches: Evidence from U.S. Higher Education Institutions.*Social Science Research Network,* 1–19.http://penghuang.com/WordPress/wp-content/uploads/2021/01/IT-Centralization- Security-Outsourcing-and-Cybersecurity-Breach.pdf

Lundholm, K., Hallberg, J., &Granlund, H. (2011).Design and use of information security metrics.*FOI, Swedish Def. Res. Agency, p. ISSN*, 1650–1942.

Lynn, A. (2018, December 17). *Cyber Attacks History In Higher Education* [Information Security]. Information Security Buzz. https://www.informationsecuritybuzz.com/articles/cyber-attacks-history-in-higher-education/ [Accessed 8 Apr. 2020]

Maple, C. (2017). Security and privacy in the internet of things. *Journal of Cyber Policy*, *2*(2), 155–184. https://doi.org/10.1080/23738871.2017.1366536

Magutu, P., Ondimu, G., & Ipu, C. (2016). Effects of Cybercrime on State Security:Types, Impact and Mitigations with the Fiber Optic Deployment In Kenya. *Journal of Information Assurance & Cybersecurity*, 1–20. https://doi.org/10.5171/2011.618585

Mateti, P. (2007). *Chapter 1 Security Issues in the TCP/IP Suite*. https://doi.org/10.1142/9789812770103_0001

Maynard, P., McLaughlin, K., &Sezer, S. (2020). Decomposition and sequential-AND analysis of known cyber-attacks on critical infrastructure. *Journal of Cybersecurity*, *6*(1).https://doi.org/10.1093/cybsec/tyaa020

McCarthy, J. (2018). *Academia under Siege*.*19*(3).https://doi.org/10.1007/s12045-014-0027-9

Miller, E. (2022). *The State of Higher Education Cybersecurity: Top Insights and Trends* (Secure Your Cyber Security through Tough Ecnomic Times, p. 12) [Annual]. https://www.bitlyft.com/resources/the-state-of-higher-education-cybersecurity-insights-trends

Morris, E. (2015). Sampling from Small Populations. *University of Regina*. https://uregina.ca/~morrisev/Sociology/Sampling%20from%20small%20populations.htm

Muchira, N. (2018, April 27). *Governments and financial institutions worry as Africa loses $3.5b to cyber-crime*. The East African.https://www.theeastafrican.co.ke/tea/business/governments-and-financial-institutions-worry-as-africa-loses-3-5b-to-cyber-crime-1392408 [Accessed 6 Jul. 2019]

Muendo, M. (2019, December 2). *What's been done to fight cybercrime in East Africa* [Academic Rigour, Journalistic Flair].The Conversation.http://theconversation.com/whats-been-done-to-fight-cybercrime-in-east-africa-127240 [Accessed 4 Oct. 2019]

MUIRURI, K. (2019, May 14). *Cyber threats cost Kenyan economy Ksh. 25.9B in 2018—Report* [National Broadcaster Digital Platform]. Citizentv.Co.Ke. https://citizentv.co.ke/business/heightened-cyber-risks-cost-economy-ksh-25-9-billion-report-247593/ [Accessed 14 Oct. 2019]

Munguti, R. (2020, October 27). *JKUAT students charged with hacking bank, stealing millions | Nation* [National Daily Digital Print]. Nation.https://nation.africa/kenya/news/jkuat-students-charged-with-hacking-bank-2722762?view=htmlamp&__twitter_impression=true [Accessed 4 Jan. 2021]

Ndiege, J. R. A., &Okello, G. O. (2018).*Information security awareness amongst students joining higher academic institutions in developing countries: Evidence from Kenya*. *10*(3), 19.https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=1555&context=ajis [Accessed 4 Jun. 2021]

Nicol, J. (2020, May 6). *York University Hacked: What We Know So Far*. Medium. https://medium.com/@jamienicol97/york-university-hacked-what-we-know-so-far-e5eb9c03b030 [Accessed 14 Oct. 2019]

Ncube, C., & Garrison, C. (2010). Lessons learned from university data breaches. *Palmetto Business & Economic Review*, *13*, 27–37.

Ochieng, O. C. (2014). THE MAJOR ELEMENTS FOR INFORMATION TECHNOLOGY SECURITY MANAGEMENT IN UNIVERSITIES IN KENYA. *International Journal Of Social Sciences and Information Technology*. https://d1wqtxts1xzle7.cloudfront.net/57773394/The_Major_Elements_For_Information_Technology_Security_Management_In_Universities_In_Kenya.pdf?1542268699=&response-content-disposition=inline%3B+filename%3DThe_Major_Elements_For_Information_Techn.pdf&Expires=1618423367&Signature=Guz8mLDoIUo2TRyarxxgPUI86ugbPzn~l2Q7cG0HzA0PbIil~v6BApXZzZwMneDTN1yFjrBt5wJTZToBesO6nL7wYIfBE0kFSbpPDxXq94TWSh6Fv~Omu9NubaHh8i2WNO5qYQ4zxjtal19WdcaHJgbC1yvMqQRRdNBL17GW5It-B9tzDMkdlTuZXxd6p34k6mUoQ8nf8cq0Pz-wuPkNajY-UesHTcAS6nOXCQ2mk8U6JVzjJnWE1bHmX1uh047~VVUGZFh4Ae-vpAzwn48a8eIntxgrQMmgjrcH8SmPwWs200ARH52QPSTcOXillUc4koL4nUTQugpp2eCJT5hRlg__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA [Accessed 4 Dec. 2020]

Odhiambo, G. O. (2011). Higher education quality in Kenya: a critical reflection of key challenges. *Quality in Higher Education*, *17*(3), 299–315. https://doi.org/10.1080/13538322.2011.614472

Oblinger, D. (2020, August). Digital Transformation: It's Time. *EDUCAUSE*.https://er.educause.edu/articles/2020/8/digital-transformation-its-time

Olalere, M., Abdullah, M., Mahmod, R., & Abdullah, A. (2015). A Review of Bring Your Own Device on Security Issues. *SAGE Open*, *5*. https://doi.org/10.1177/2158244015580372

Ondersma, S. J., Martino, S., Svikis, D. S., & Yonkers, K. A. (2017). Staying focused on non-treatment seekers. *Addiction (Abingdon, England)*, *112*(5), 828–829. https://doi.org/10.1111/add.13736

Oxford-Mail. (2017, September 5). *Hundreds of potential cyber-attacks a year on Oxford University "repulsed"* [University Digital News Paper]. Oxford Mail.https://www.oxfordmail.co.uk/news/15515897.hundreds-potential-cyber-attacks-year-oxford-university-repulsed/ [Accessed 4 Oct. 2019]

Pandey, S. (2016). MODERN NETWORK SECURITY: ISSUES AND CHALLENGES. *International Journal of Engineering Science and Technology*, *3*.

Pagliery, J. (2015, July 17). *UCLA Health hacked, 4.5 million victims*. CNNMoney.https://money.cnn.com/2015/07/17/technology/ucla-health-hack/index.html [Accessed 4 Sep. 2019]

Pawar, M. V., &Anuradha, J. (2015).Network Security and Types of Attacks in Network.*Procedia Computer Science*, *48*, 503–506.https://doi.org/10.1016/j.procs.2015.04.126

Perlroth, N. (2015, May 15). Penn State's College of Engineering Hit by Cyberattack.*Newyork Times*.https://www.nytimes.com/2015/05/15/penn-states-college-of-engineering-hit-by-cyberattack/

Perlroth, N. (2013, January 31). Hackers in China Attacked The Times for Last 4 Months. *The New York Times*. https://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html [Accessed 25 Nov. 2020]

Pérez-Peña, R. (2013, December 4). Student Debt Load Found to Vary by College and State—The New York Times. *The New York Times*.https://www.nytimes.com/2013/12/05/education/student-debt-load-varies-greatly-by-college-and-region.html [Accessed 26 Oct. 2019]

Pirani, J. A., &Yanosky, R. (2007). Shelter from the storm: IT and business continuity in higher education. *EDUCAUSE Center for Applied Research Bulletin*.

Press, S. J., & Wilson, S. (1978). Choosing between logistic regression and discriminant analysis. *Journal of the American Statistical Association*, *73*(364), 699–705.

Price Waterhouse Cooper (2012), Business continuity management, retrieved fromhttps://www.pwc.com/us/en/10minutes/assets/pwc-10minutes-business-continuity-management.pdf

Rahim, N. (2021). *Bibliometric Analysis of Cyber Threat and Cyber Attack Literature: Exploring the Higher Education Context*. IntechOpen.https://doi.org/10.5772/intechopen.98038

Rajaraman, V. (2014).Artificial intelligence & Higher Learning.*Resonance*, *19*(3), 198–207.https://doi.org/10.1007/s12045-014-0027-9

Rao, U. H., &Nayak, U. (2014).Understanding Networks and Network Security. In U. H. Rao& U. Nayak (Eds.), *The InfoSec Handbook: An Introduction to Information Security* (pp. 187–204). Apress.https://doi.org/10.1007/978-1-4302-6383-8_9

Ravali, P. (2014). A Comparative Evaluation of OSI and TCP/IP Models. *International Journal of Science and Research (IJSR), 4*(7), 514–521. https://www.ijsr.net/get_abstract.php?paper_id=SUB155737

Readhead, A. C. S., Taylor, G. B., Xu, W., Pearson, T. J., Wilkinson, P. N., & Polatidis, A. G. (1996). The statistics and ages of Compact Symmetric Objects. *The Astrophysical Journal*, *460*, 612.

REMS.(2017). *Cybersecurity Considerations for Institutions of Higher Education*. 11.

Ridder, H.-G. (2014). Book Review: Qualitative Data Analysis. A Methods Sourcebook. *German Journal of Human Resource Management*, *28*(4), 485–487. https://doi.org/10.1177/239700221402800402

Ryerson University. (2019). *Defending universities from cyber-attacks—Can we do better?* (p. 1-3). Ryerson University.https://www.ryerson.ca/ryerson-works/articles/behind-the-scenes/2019/defending-universities-from-cyber-attacks-can-we-do-better [Accessed 4 Jun. 2021]

Salkind, N. J. (2006). *Encyclopedia of measurement and statistics*. SAGE publications. SattarovaFeruza, Y., & Kim, T. (2007). IT security review: Privacy, protection, access control, assurance and system security. *International Journal of Multimedia and Ubiquitous Engineering*, *2*(2), 17–32.

Salkind, N. J., & Rainwater, T. (2006). *Exploring research*. Pearson Prentice Hall Upper Saddle River, NJ.

Sawahel, W. (2020, June 8). *COVID-19 brings new cyber-security threats to universities*. University World News.https://www.universityworldnews.com/post.php?story=20200607084916387 [Accessed 4 Dec. 2020]

Schaffer, F. P. (2014). A Guide to Academic Freedom.*Collective Bargaining in the Academy*, *0*, 54.https://thekeep.eiu.edu/cgi/viewcontent.cgi?article=1325&context=jcba

Scheer, A. W., Abolhassan, F., Jost, W., &Kirchmer, M. (2004).*Business process automation*. Heidelberg: Springer.

Shakoor, F., & Abbas, J. (2021). Impact of Smartphones Usage on the Learning Behaviour and Academic Performance of Students: Empirical Evidence from Pakistan. *International Journal of Academic Research in Business and Social Sciences, 11*. https://doi.org/10.6007/IJARBSS/v11-i2/8902

Sarraf, S. (2019, December 16). *Education sector is the most vulnerable to cloud attacks*. CIO.https://www.cio.com/article/3490410/education-sector-is-the-most-vulnerable-to-cloud-attacks.html [Accessed 24 Dec. 2020]

Serianu. (2012). *SERIANU: Kenya Cyber Report 2012* (Nattional Cyber Security Status No. 1; Getting Back To Security Basics, pp. 1–32). Serianu Limited. https://www.serianu.com/downloads/KenyaCyberSecurityReport2012.pdf

Standard Group PLC. (2020, September).*Securing African Universities from cyber threats* [Daily Newspaper Digital print]. The Standard.https://www.standardmedia.co.ke/author/dr-bright-gameli-mawudor [Accessed 4 Dec. 2020]

Symantec.(2014). *2014 Internet Security Threat Report* (Annual No. 19; ISTR 2013 Trends, p. 100).https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Symantec_annual_internet_threat_report_ITU2014.pdf [Accessed 4 Jan. 2017]

Symantec. (2015). Attackers Are Moving Faster, Defenses Are Not. Internet Security Threat Report, 20, 5-6.

Symantec. (2016). *2016 Internet Security Threat Report* (Annual No. 21; p. 82).Symantec.https://www.insight.com/content/dam/insight-web/en_US/article-images/whitepapers/partner-whitepapers/Internet%20Security%20Threat%20Report.pdf [Accessed 4 Jan. 2017]

Task Force Transformation Initiative. (2012). *Guide for Conducting Risk Assessments* (NIST Special Publication (SP) 800-30 Rev. 1). National Institute of Standards and Technology.https://doi.org/10.6028/NIST.SP.800-30r1 [Accessed 4 Aug. 2019]

Tidy, J. (2020, July 24). Blackbaud hack: More UK universities confirm breach. *BBC News*. https://www.bbc.com/news/technology-53528329

Tongco, M. D. C. (2007). *Purposive sampling as a tool for informant selection*.

Tushabe, F., &Baryamureeba, V. (2005). Cyber Crime in Uganda: Myth or Reality? *World Academy of Science, Engineering and Technology*, *8*, 5.

Tzenev, I., Popov, G., &Shirkova, M. (2015). RISK ASSESSMENT MODEL BASED ON ISO 22301:2012 "SOCIETAL SECURITY. BUSINESS CONTINUITY MANAGEMENT SYSTEMS.REQUIREMENTS."*Materials, Methods & Technologies*, *9*(1), 531–540. https://www.scientific-publications.net/en/article/1000801/

UNIT.(2019). *Unit-Department for ICT and Joint Services in Higher Education and Research.* (p. 1-14). https://www.regjeringen.no/contentassets/f464322e9623456dabe220571dfab8f6/unit-okonomiseminar_2019.pdf

Universities UK. (2013). Cyber Security and Universities: Managing the Risk. UniversitiesUK, 5-6.

universityworldnews. (2012, September 2). *Two universities hit by Anonymous cyber-attack* [University News Letter]. University World News.https://www.universityworldnews.com/post.php?story=20120831195643360 [Accessed 29 Dec. 2020]

Verizon. (2016). *2016 Data Breach Investigations Report* (Annual No. 9; 89% of Breaches Had a Financial or Espionage Motive, pp. 1–85). https://cybersecurity.idaho.gov/wp-content/uploads/sites/87/2019/04/DBIR_2016_Report.pdf [Accessed 24 Nov. 2019]

Verizon.(n.d.).*Verizon's 2016 Data Breach Investigations Report finds cybercriminals are exploiting human nature*. Retrieved April 11, 2021, from https://www.prnewswire.com/news-releases/verizons-2016-data-breach-investigations-report-finds-cybercriminals-are-exploiting-human-nature-300258134.html [Accessed 14 Nov. 2019]

Vogel, V. (2015).Information security aspects of business continuity management.

: https://spaces.internet2.edu/display/2014infosecurityguide/Information Security Aspects

Of Business Continuity Management [Accessed April 10th 2015]

Wagstaff, K., &Sottile, C. A. (2015, September 20). *Cyberattack 101: Why Hackers Are Going After Universities*. https://www.nbcnews.com/tech/security/universities-become-targets-hackers-n429821

Wangen, G. B., &Ulven, J. (2021).A Systematic Review of Cybersecurity Risks in Higher Education.*Future Internet*, *13*.https://doi.org/10.3390/fi13020039

Wasonga, M. (2019, March 13). *cybersecurity for schools ahead of East Africa's Cloud and Security Summit*. CIO East Africa.https://www.cio.co.ke/serianu-hosts-a-cybersecurity-fair-for-schools-ahead-of-east-africas-cloud-and-security-summit/ [Accessed 1 Nov. 2018]

Xu, S., Zhou, Y., Guo, R., Du, J., & Liu, Z. (2019). A security model based on intelligent decision. *Journal of Physics: Conference Series*, *1187*(4), 042039. https://doi.org/10.1088/1742-6596/1187/4/042039

.Yilmaz, R., &Yalman, Y. .(2016). A Comparative Analysis of University Information Systems within the Scope of the Information Security Risks.*TEM J.*, *5*, 180–191.

York, D. (2010). CHAPTER 3 - Eavesdropping and Modification. In D. York (Ed.), *Seven Deadliest Unified Communications Attacks* (pp. 41–69). Syngress.https://doi.org/10.1016/B978-1-59749-547-9.00003-X [Accessed 20 Dec. 2020]

7. APPENDICES

Appendix 1: Letter from Board of Postgraduate Studies

JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE & TECHNOLOGY

BOARD OF POSTGRADUATE STUDIES

Office of the Director

Tel. 057-2501804
Email: bps@jooust.ac.ke

P.O. BOX 210 - 40601
BONDO

Our Ref: **I152/4056/2014** **Date**: Tuesday, December 6, 2016

TO WHOM IT MAY CONCERN

RE: JEREMIAH OYANA OWANGO – I152/4056/2014

The above person is a bona fide postgraduate student of Jaramogi Oginga Odinga University of Science and Technology in the School of Informatics & Innovative Systems pursuing Masters Degree. He has been authorized by the University to undertake research on the topic: **"Cyber-Attack on Business Continuity in Universities in Kenya".**

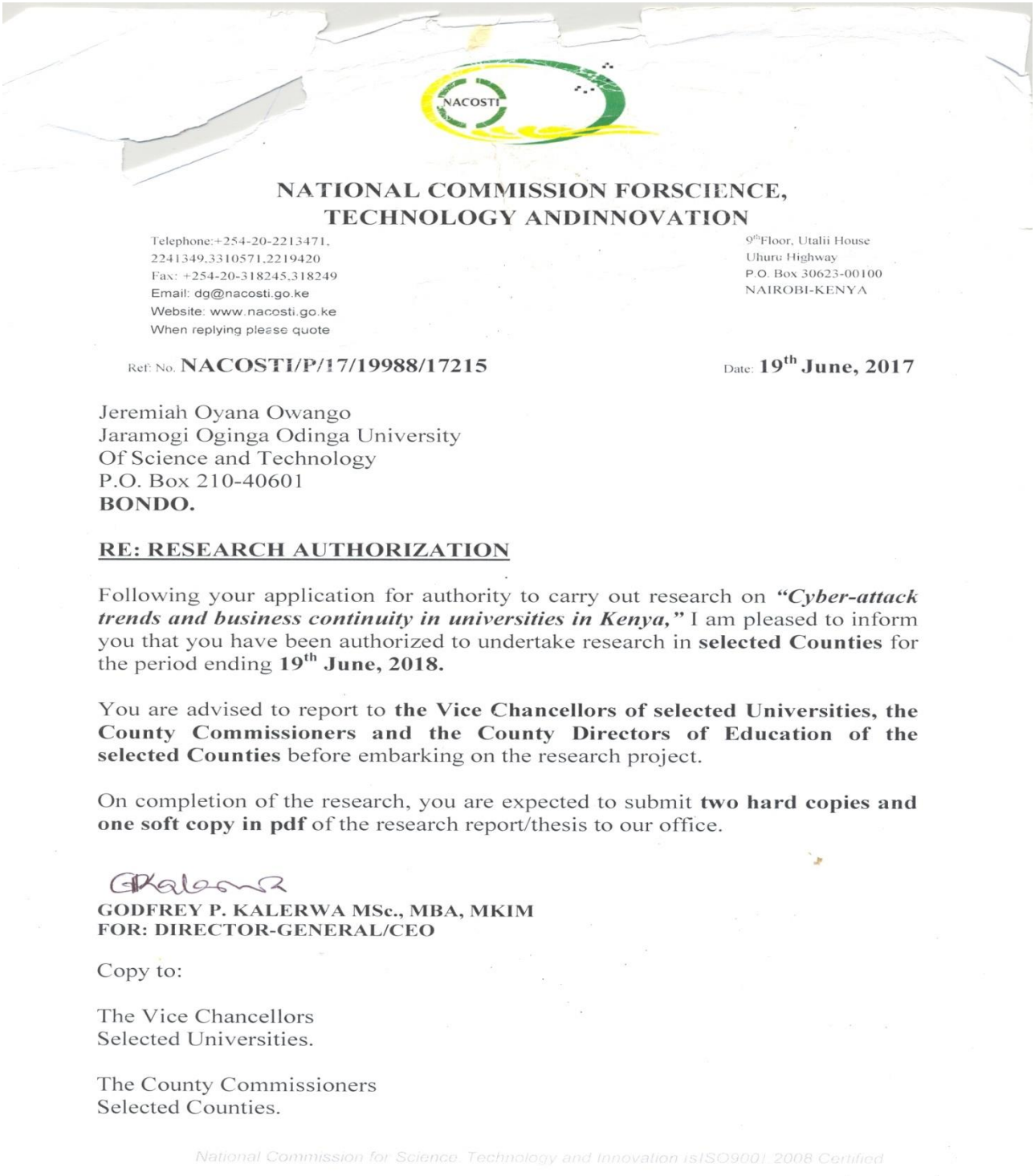
Any assistance accorded to him shall be appreciated.

Thank you.

Prof. Beatrice Anyango
DIRECTOR, BOARD OF POSTGRADUATE STUDIES

cc. Dean, SIIS

Appendix 2: Letter of Authorization from National Research Council



NATIONAL COMMISSION FORSCIENCE,
TECHNOLOGY ANDINNOVATION

Telephone:+254-20-2213471,
2241349,3310571,2219420
Fax: +254-20-318245,318249
Email: dg@nacosti.go.ke
Website: www.nacosti.go.ke
When replying please quote

9th Floor, Utalii House
Uhuru Highway
P.O. Box 30623-00100
NAIROBI-KENYA

Ref: No. **NACOSTI/P/17/19988/17215**

Date: **19th June, 2017**

Jeremiah Oyana Owango
Jaramogi Oginga Odinga University
Of Science and Technology
P.O. Box 210-40601
BONDO.

RE: RESEARCH AUTHORIZATION

Following your application for authority to carry out research on ***"Cyber-attack trends and business continuity in universities in Kenya,"*** I am pleased to inform you that you have been authorized to undertake research in **selected Counties** for the period ending **19th June, 2018.**

You are advised to report to **the Vice Chancellors of selected Universities, the County Commissioners and the County Directors of Education of the selected Counties** before embarking on the research project.

On completion of the research, you are expected to submit **two hard copies and one soft copy in pdf** of the research report/thesis to our office.

GODFREY P. KALERWA MSc., MBA, MKIM
FOR: DIRECTOR-GENERAL/CEO

Copy to:

The Vice Chancellors
Selected Universities.

The County Commissioners
Selected Counties.

National Commission for Science, Technology and Innovation is ISO9001: 2008 Certified

Appendix 3: SWOT analysis of Network Models and Network Security Models

SWOT Analysis of OSI Model, (Danesh, 2021)

Strength	Weakness
1. Generic model used on any type of network that provides guidance in development for any computer network. 2. Ensure interoperability of technology. 3. Flexibility- enables connection-oriented services or connectionless services. 4. Layered architecture that provides separation for each layer which protects each layer from affecting another.	1. Theoretical and does not provide satisfactory clarification for practical network development. 2. Inappropriate time of launch that made it considered inferior to TCP/IP. 3. It is a complex model; preliminary implementation was gradual, prohibitive and cumbersome 4. Practical application is limited; does not full consider accessibilities of appropriate technologies. 5. Duplicated services in some layers eg error control, flow control and addressing.
Opportunities	**Threats**
1. Beneficial external factors; ability to redefine all the rules and standards in accordance with modern knowledge.	1. Internal Threats: individuals within an organization who is knowledgeable in organization security procedures and capitalizes on the loop holes. 2. External threats : Competing models created in future, competing models like TCP/IP

SWOT Analysis of TCP/IP Model, (Ravali, 2014).

Strength	Weakness
1. Industry standard that can be	1. Not generic in nature; fails to

deployed in practical networking problems. 2. Interoperable; allows cross platform communication among heterogeneous networks. 3. Open protocol suite ie not owned by one particular institute. 4. Scalable client server architecture ie network can be expanded without disrupting current services. 5. Automatically assign link local address on systems on networks. 6. Assign IP address on devices on networks. 7. Reliable and flexible	represent any protocol suite other than TCP/IP 2. Not suitable to describe new technologies; does not clearly separate concept of services, interfaces and protocols. 3. Does not distinguish between data link and physical layers which have very different functionalities 4. Designed for WAN not optimized for small networks like LANs or PANs. 5. Some protocols were developed ad hoc and proved unsuitable in the long run
Opportunities	**Threats**
1. IP is an evolving protocol	1. Port Scanning, man in the middle, DoS/DDoS, IP Spoofing, DNS Spoofing

SWOT Analysis of Network Security Model (NSM), (Kizza et al., 2013).

Strength	**Weakness**
1. The private key used in the encryption is robustly resistant to brute force attacks. 2. Secret key algorithm requires less computing power to be created.	1. Necessity for a proper exchange of private keys. 2. Additional users getting private keys compromises existing private keys since if one private key is compromised all private keys are compromised. 3. It addresses only transmission aspect of networks.

Opportunities	**Threats**
1. Evolution of computing power creates stronger crypto hashes at a shorter time.	1. Compromise of private keys

SWOT Analysis of Network Access Security Model (NASM), (Blackfield & Bambernek, 2021)

Strength	**Weakness**
1. Addresses most weaknesses inherent in OSI, TCP/IP models. 2. Consider the user aspect in security	1. Does not address active monitoring of networks 2. Lack an IDS/IPS Layer 3. Model is not full proof
Opportunities	**Threats**
1. Can be used to implement some OSI model weaknesses 2. Can be used to implement some TCP/IP weaknesses 3. Its malleable, it can be adopted in various organizations for a variety of network security scenarios.	1. It is a generic model 2. Fail to address active treats 3. It is still new, it's not been proven

SWOT Analysis of Privacy Preserving Demand Response (P2DR) Model, (Liu et al., 2010)

Strength	**Weakness**
1. Breaks down security measures into four distinct aspects of; 2. Protection; phase includes set of strategies, products and processes designed to prevent the success of attack. 3. Detection; goal is to reduce the time it takes to identify threats.	1. Industry generic model; not specific ICT security

4. Response; deal with discovered threats in a timely manner 5. Recovery; repair the damage caused by the attack	
Opportunities	**Threats**
1. As its generic it can be utilized in any industry. 2. It can be used as a template for other models to improve on.	1. Internal Threats: individuals within an organization who is knowledgeable in organization security procedures and capitalizes on the loop holes

Appendix 4: Questionnaire

This questionnaire is meant to collect data on network security status among university ICT personnel in Kenya. The main purpose of the data that will be collected is to develop a theoretical model that will govern network security implementation in universities in the country. Your responses will be treated in strict confidence. Please answer all questions as accurately as you can.

This questionnaire will take a few minutes of your time - Thank You.

Section One

Respondent general characteristics

a) How long have you served in the institution?

- ❒ 6 months to 1 year
- ❒ 1 Year to 3 years
- ❒ More than 3 years

b) What is the student population in your institution?

- ❒ Below 5, 000
- ❒ Between 5, 000 and 15, 000
- ❒ Over 15, 000

c) What position is held by the individual who manages network security in your institution?

- ❒ Network Administrator
- ❒ System Administrator
- ❒ Security specialist
- ❒ None
- ❒ Don't Know

Section Two

Question One

a) Are you aware of network models used in your institution?

☐ Yes

☐ No

b) If yes to the above; what network model is used in your institution?

❒ TCP/IP

❒ OSI

❒ Don't Know

❒ None

c) Are you aware of the inherent weaknesses of the model chosen above?

❒ Strongly Agree

❒ Agree

❒ Neutral

❒ Disagree

❒ Strongly Disagree

d) What network security model is used to counter the weakness of the network model in your institution?

❒ Network Access Security Model (NASM)

❒ Network Security Model (NSM)

❒ Protection, Detection, Recovery Model (P2DR)

❒ Don't Know

❒ None

e) Are you aware of the inherent weaknesses of the security model chosen above?

❒ Strongly Agree

❒ Agree

❒ Neutral

❒ Disagree

❒ Strongly Disagree

f) In your opinion does the selected security model adequately secure the institution network?

❒ Strongly Agree

❒ Agree

❒ Neutral

❒ Disagree

❒ Strongly Disagree

2. Is your institution network part of a larger network? (ie does it support satellite campuses)

❒ Strongly Agree

❒ Agree

❒ Neutral

❒ Disagree

❒ Strongly Disagree

3. Is your entire institution network centrally managed?

❒ Strongly Agree

❒ Agree

- ❒ Neutral
- ❒ Disagree
- ❒ Strongly Disagree

Question Two

1. Answer the following questions to the best of your knowledge

Key

Network Access Security Model (NASM)

Network Security Model (NSM)

Privacy Preserving Demand Response (P2DR) Model

Which network security model?

No	Variable	NASM	NSM	P2DR	None	Don't Know
1	Is utilized in your institution?					
2	Addresses external access to the internal secure network?					
3	Addresses firmware and network security patching?					
4	Utilizes Network Address Translation (NAT), Virtual LAN (VLAN), Virtual Private Networks (VPN) used in your institution network?					
5	Emphasizes segmentation of the network?					
6	Addresses defects in network applications?					
7	Encourages inventory of authorized and unauthorized					

	devices on the network?					
8	Addresses network recovery capabilities?					
9	Addresses secure network configurations?					
10	Prioritize most critical network assets?					

2. Please answer the following questions with respect to the Network Security Model used in your institution;

a) Network Access Security Model (NASM)

No	Variable	SA	A	N	D	SD
1	Has your institution put in place measures to correct weaknesses of the network model used?					
2	Is IPS/IDS used on the institution network?					
3	Is active monitoring utilized on your institution network					
4	Is passive monitoring utilized on your institution network					
5	Is internet access to the network is regulated via proxy relays?					
6	Is encryption of data in transit and storage enabled on your network?					
7	Emphasize security zones with different levels of security within the network?					

b) Network Security Model (NSM)

No	Variable	SA	A	N	D	SD

1	Has your institution put in place measures to correct weaknesses of the network model used?					
2	Is IPS/IDS used on the institution network?					
3	Is active monitoring utilized on your institution network					
4	Is passive monitoring utilized on your institution network					
5	Is internet access to the network is regulated via proxy relays?					
6	Is encryption of data in transit and storage enabled on your network?					
7	Emphasize security zones with different levels of security within the network?					

c) Privacy Preserving Demand Response (P2DR) Model

No	Variable	SA	A	N	D	SD
1	Has your institution put in place measures to correct weaknesses of the network model used?					
2	Is IPS/IDS used on the institution network?					
3	Is active monitoring utilized on your institution network					
4	Is passive monitoring utilized on your institution network					
5	Is internet access to the network is regulated via proxy relays?					

6	Is encryption of data in transit and storage enabled on your network?					
7	Emphasize security zones with different levels of security within the network?					

Question Three

a) What factors do you believe affect implementation of network security and in your institution?

Variable	SA	A	N	D	SD
Unrestricted access of information within university					
Collaboration with other Institutions/Organizations					
Highly technical and unpredictable student population					
Large number of legacy systems in use in the institution					
BYOD is encouraged					
BYOD is managed in the institution					

b. What percentage of the institution network (including satellite campuses) does the university ICT department manage and control?

- ❒ 0% of the institution
- ❒ 25% of the institution
- ❒ 50% of the institution
- ❒ 75% of the institution
- ❒ 100% of the institution

1. Does your institution have control over the devices that students and faculty use on campus?

❒ Strongly Agree

❒ Agree

❒ Neutral

❒ Disagree

❒ Strongly Disagree

2. Is access to information restricted within the institution's networks?

❒ Strongly Agree

❒ Agree

❒ Neutral

❒ Disagree

❒ Strongly Disagree

3. Are network users educated on network hygiene?

❒ Strongly Agree

❒ Agree

❒ Neutral

❒ Disagree

❒ Strongly Disagree

4. Does your institution use legacy information systems older than ten years?

☐ Strongly Agree

☐ Agree

☐ Neutral

☐ Disagree

☐ Strongly Disagree

5. Does your institution have collaborations with other institutions/organizations?

❒ Yes

❒ No

(a)If yes, what is the nature of these collaborations?

☐ Academic

☐ Research and innovation

☐ Research and development

☐ Exchange of ideas

(b) If yes, what types of collaborations?

☐ Within academic institution (Academic researchers within institution)

☐ Between academic institutions

☐ Between institution and government agencies

☐ Between institution and private agency

☐ Between institution and international partners

6. Do the institution collaboration partners access the universities network securely?

❒ Strongly Agree

❒ Agree

❒ Neutral

❒ Disagree

❒ Strongly Disagree

6. Do you consider your network users unpredictable?

   - ❒ Strongly Agree
   - ❒ Agree
   - ❒ Neutral
   - ❒ Disagree
   - ❒ Strongly Disagree

7. Do you consider your local area network users a threat to networks security?

   - ❒ Strongly Agree
   - ❒ Agree
   - ❒ Neutral
   - ❒ Disagree
   - ❒ Strongly Disagree

8. Do you consider your local area network users as technically competent Internet users?

   - ❒ Strongly Agree
   - ❒ Agree
   - ❒ Neutral
   - ❒ Disagree
   - ❒ Strongly Disagree

9. If yes to the above, does your institution's network frequently get compromised internally?

   - ❒ Strongly Agree
   - ❒ Agree
   - ❒ Neutral

❒ Disagree

❒ Strongly Disagree