UNIVERSITY OF NAIROBI

SCHOOL OF COMPUTING AND INFORMATICS

FRAMEWORK FOR EFFECTIVE MANAGEMENT OF CYBER SECURITY ON E-LEARNING PLATFORMS IN PUBLIC UNIVERSITIES IN KENYA

RONALD BARASA CYOY

RESEARCH PROJECT REPORT SUBMITTED TO THE DEPARTMENT OF COMPUTING AND INFORMATICS IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT OF THE UNIVERSITY OF NAIROBI

JANUARY 2022

DECLARATION

This project report to the best of my knowledge is my original work and has not been submitted for any other award in any University.

Signature: Date: 28.01.2022

Student Name: Ronald Barasa Cyoy

Registration Number: P54/32965/2019

This project report has been submitted for examination with my approval as University Supervisor

Signature: Date: 09/03/2022

Prof. Elisha Omulo Opiyo

Department of Computing and Informatics

University of Nairobi

DEDICATION

I’d like to dedicate this work to my family for their love and continuous support throughout my journey. To my children Raymond and Mark who have been affected by my absence due to this quest which has been time consuming.

ACKNOWLEDGEMENT

I would like to thank the Almighty God for sustaining me and giving me strength throughout this Journey. My sincere gratitude goes to my Supervisor, Prof. Elisha Opiyo Omulo, for his fatherly guidance, support, time and invaluable contribution to ensure success of this project. I appreciate the panelist for their review of this project to ensure that it meets the threshold. Last but not list I take this opportunity to thank the Department of computing & informatics and my colleagues especially Simon Njuguna and Wambui Waithaka for their concerns to ensure that I complete my Masters. Grateful thanks to University of Nairobi fraternity for giving me the opportunity to pursue Master of Science in Information Technology Management. Thankyou God bless you all.

ABSTRACT

Many institutions of higher learning in Kenya are adopting e-learning platforms and like other popular online platforms e-learning allows for extensive exchange of information via the internet and therefore provides fertile grounds for cybercrime. Some e-learning systems supporting online collaborative learning do not sufficiently meet essential security requirements where students can falsify course assessments, present a convincing false identity to others, alter date stamps on submitted work among other cybersecurity issues. This calls for an effective way to manage cybersecurity on e-learning platforms. The review of various scholarly sources identified an existing gap, which pointed to a deficiency of a framework to manage cybersecurity on e-learning systems. This study sought to fill the knowledge gap by adopting features borrowed from K-12 Cyber protection Framework. To address the identified problem, the research was carried out at the three selected public chartered universities in Kenya with focus on in-depth understanding the management of cybersecurity on e-learning platforms. Questionnaires composed of Likert scale were used to collect data where 90 participants were conducted during the study. The data was analyzed using descriptive and regression analysis where the results and findings highlighted that identity, protection, detection, response, user skills and compliance had significant influence on effective management of cybersecurity on e-learning platforms. The research recommended sensitization programs for users and the compliance on regulations established to reduce vulnerabilities.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

CIA	Confidentiality, Integrity and Availability
COBIT	Control Objectives for Information and related Technology
IT	Information Technology
ICT	Information and communications technology
IS	Information System
ISMS	Information Security Management System
ISM	Information Security Management
LMS	Learning Management System
MOODLE	Modular Object-Oriented Dynamic Learning Environment
NIST	National Institute of Standards and Technology
OIPT	Organizational Information Processing Theory
OSMS	Open Source Management Systems
TTF	Task Theory Fit
KENET	Kenya Education Network
FBI	Federal Bureau Investigation
BYOD	Bring Your Own Device
IC3	Crime Complaint Center
PwC	Price Water House Coopers
SCADA	Supervisory Control and Data Acquisition
IFMIS	Integrated Financial Management Information system
VDs	Virtualized Desktops
LMS	Learning Management System ()
ISO	International Organization for Standardization
CPF	Cyber Protection Framework
EJEL	The Electronic Journal for E-learning
IJEDE	International Journal of E-Learning and Distance Education
VIF	Variance Inflation Factors
PKI	Public Key Infrastructure
CIMS	Certified Information Security Management
OTP	One-Time Passwords

SMTP	Simple Mail Transfer Protocol
SPSS	Statistical Packages for Social Sciences Version 24

DEFINITION OF TERMS

E-Learning: Is the acquisition and use of knowledge distributed and facilitated primarily by electronic means through the Multi-media, Tele-learning, the Flexible Learning and the Intelligent Flexible Learning Models.

Cybercrime: It involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target.

Cyber Risk: Exposure to harm or loss resulting from breaches of or attacks on information systems.

Cybersecurity: Is the body of technologies, processes, and practices designed to protect networks, computers, programs and data from attack, damage, or unauthorized access.

E-mail: E-mail (short for electronic mail; often also abbreviated as e-mail, email or simply mail) is a store and forward method of composing, sending, storing, and receiving messages over electronic communication systems. The term "e-mail" (as a noun or verb) applies both to the Internet e-mail system based on the Simple Mail Transfer Protocol (SMTP) and to intranet systems allowing users within one organization to e-mail each other.

Online: An adjective for describing the state of an object connected to the internet. If the object is online, it is accessible through the Internet.

CHAPTER ONE

INTRODUCTION

1.1 Background to the Problem

ICTs Proliferation with internet connectivity in the Country has seen widespread use and adoption of the same in public, private entities and individuals for use in a wide range of activities. ICT infrastructure has been widely adopted by government organizations as well as private entities owing to the exponential ease of processes in commerce, manufacturing, education, research and development, delivery of services, enhancing accountability and efficiency among others (Chairoel, Widyarto & Pujani, 2015), (Ratheeswari, 2018).

ICTs' extensive application in Education has led to enhancement of teaching & learning through advanced tools. Numerous studies carried out to access how institutions of higher learning in Kenya are prepared to accept and apply online platforms to promote learning. The results indicated that many institutions were slowly piloting the platforms. Unfortunately, internet has become a new sphere for cyber-crime where information associated with organizations, institutions; personal, protected or confidential information is exposed to security threats emanating from cyber criminals. Sir Timothy Berners-Lee (2019), advocated for concerted efforts to address insecurity in the internet, stating that criminals to propagate their heinous activities have abused it.

Bazimaziki,(2020), observes that many institutions of higher learning globally, regionally and locally have embraced various technologies; particularly in e-learning which has grown rapidly during the Covid-19 pandemic. E-learning has enabled continuity of learning during this season, where it has reduced health risks associated with covid-19. However, the extensive use of these online platforms makes them a big target to cyber criminals just like other ICT platforms. Symantec's (2015), showed that (10%) of cyber threats witnessed globally targeted learning institutions.

Swiatkowska, J. (2020), avers that cybercriminals have used internet to commit various crimes not limited to; cases of unauthorized access, to disinformation spreaders, online fraud, scams, organized crimes, terrorist activities and illegal trade. Currently, cybersecurity is key in safeguarding the ever-changing world. Europol report (2018) asserts that with the emergence of new technologies such as IoT poses equally new challenges in addressing threats emanating from the same. Similarly, the entry of 5G networks, which allows users to download data from multiple sources simultaneously at lower latency and higher throughput, will make investigation of communication events complex (Europol, 2018).

Carliner & Shank (2016) notes that proliferation of e-learning technologies in Education sector, has brought myriad of challenges to traditional system administrators who are used to managing proprietary systems, adding that the new technologies support multiple users and requires regular upgrades to address cyber threats emanating from the same. Camino Kavanagh(2019), asserts that e-learning systems are fairly cool to utilize which makes them susceptible to misuse by cybercriminals who are anonymous and can operate from anywhere anytime. Sharing data across e-learning platforms inside or outside institutions heralded to new opportunities where hackers strive for entry into networks supporting such systems (Nagy, Olah, Erdei, Mate & Popp 2018). Thus, the need for cybersecurity management on e-learning systems in institutions of higher learning.

It is worth pointing that the online systems used to provide education needs regular upgrades that sometimes when they are ignored they become vulnerable to cybercriminals. Baillette & Barlette (2018), observed that the emerging technologies like Bring-Your-Own-Device (BYOD) concept and the rise in social media applications which has been widely adopted by many students widely where they exchange a lot of personal and institutional data, has borne new security challenges that never existed before. These calls for management of cybersecurity on e-learning platforms due to increase use of such platforms and devices connecting to them.

Moore, Dickson-Deane & Galyen (2011), in their works defined e-learning as use of systems that ride on the internet to provide teaching and learning experience. In Kenya, use of online systems has been on the rise across the institutions of higher learning since the outbreak of Covid-19, which increased their cyber security risk exposure (Serianu, 2020).

These e-learning platforms share comparable features like other electronic financial platforms which makes them targets to scammers. Therefore, cybercriminals are working round the clock to ensure that they create loopholes in the same platforms for their personal gain. The Africa Cybersecurity Serianu report (2017), paints a picture of damages caused by Cyber Crimes globally and regionally. The report indicated a loss of about 3.5 billion US dollars globally and 649 million dollars in Africa.

Hollow & ICWE (2009), notes that e-learning platforms in Sub-Sahara Africa are facing challenges due to lack of frameworks, budgets, skilled users and over rated security services which have left such platforms exposed to cyberattacks.

1.2 Problem statement

Many institutions of higher learning in Kenya are adopting e-learning platforms and like other popular online platforms, e-learning allows for extensive exchange of information via the internet and therefore provides fertile grounds for cybercrime. This calls for the need for an effective way to manage cybersecurity on e-learning platforms.

Media report, the star newspaper on 2020-07-20, pointed that cyber-attacks targeted children learning using e-learning platforms with pornography, sexual harassment, violent content and intimidation. The malicious hacker attacks were reported after schools closed due to Covid-19 in March 2020 when many institutions shifted to e-learning.

Bandara, Ioras & Maher (2014), observes that some platforms in use have insufficient controls, which have led to impersonation, alteration of contents, reputation of institutions and financial loss among other cybersecurity issues. Therefore, there is an urgent need for a framework to guide and ensure proper management of cybersecurity on such systems.

Research objectives

Main goal of this research was to develop a framework for managing cyber security on e-learning platforms or environments in public chartered universities in Kenya.

1.3 Specific objectives

i) To examine the effect of identity on effective management of cybersecurity on e-learning platforms in Public Universities in Kenya

ii) To examine the effect of protection on effective management of cybersecurity on e-learning platforms in Public Universities in Kenya

iii) To examine the effect of detection on effective management of cybersecurity on e-learning platforms in Public Universities in Kenya

iv) To examine the effect of response on effective management of cybersecurity on e-learning platforms in Public Universities in Kenya

v) To establish the joint effect of user skills and user compliance on effective management of cybersecurity on e-learning platforms in Public Universities in Kenya e- learning platforms

1.4 Research Questions

Below are questions that would aid this research:

i. How does identity affect effective management of cybersecurity on e-learning platforms in Public universities in Kenya?
ii. How does protection affect effective management of cybersecurity on e-learning platforms in Public universities in Kenya?
iii. How does detection affect effective management of cybersecurity on e-learning platforms in public universities in Kenya?
iv. How does response affect effective management of cybersecurity on e-learning platforms in public universities in Kenya?
v. How does user skills and user compliance affect effective management of cybersecurity on e-learning platforms in public universities in Kenya?

1.5 Justification

More and more institutions are turning to elearning platforms to ensure that there is continuity in education. This paradigm shift is only feasible when security is guaranteed on such platforms to ensure that the content are not altered or unauthorized are not allowed to access the content. Hoog, (2015), avers that developers and vendors have often put products in the market that are not secure to cyber-attacks which contributes to nearly 90 percent of all cybersecurity exposures. It is evident that hackers rely on flaws in systems to inflict damage (Harrison and Pagliery, 2015). Cybersecurity is important to protect all data transmitted or produced from the e-learning platforms from theft and damage. Proper cybersecurity management on e-learning systems will secure sensitive data, personal information, intellectual property, personal identifiable data among other assets held therein.

Therefore, this study endeavored to narrow the existing gap by assessing current cybersecurity management practices and industry best management practices on e-learning platforms and bring new knowledge through a framework to manage cybersecurity on e-learning platforms.

Significance of the study

Inquiries about management of cybersecurity on online platforms used in public chartered universities in Kenya are scanty, despite ever-growing dependency by institutions on such systems to carry out missions and business functions. This study will assess how the cybersecurity is managed currently on e-learning platforms on the selected public universities by identifying and analyzing the gaps that exist in the current state of affairs visa vis the industry best practices which is crucial for proposing an effective framework for managing cybersecurity on e-learning platforms.

Cichonski, Millar, Grance & Scarfone, (2012), noted that there is need for mitigation strategies to be in place to address any incidences or initiate recovery plans to reduce downtime in the event of an attack.

1.6 Scope

The study was carried out in three Public Chartered Universities using e-learning platforms in Kenya. The respondents were drawn from two faculties/schools from the three universities which composed of lecturers and students using eLearning platforms as well as e-learning administrators who were informants of the study having versed knowledge on e-learning platforms as managers.

1.7 Limitations of the study

The study was based on three public chartered Universities in Kenya using E-learning platforms. For conclusive results, more public chartered universities should have been studied in the Country. However, this was not possible due to constraints experienced during the study. It was not possible to cover a larger number of courses, faculties/schools, lecturers and students' because of the prevailing Covid-19 which demanded considerable time, resources and other logistics.

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

This chapter paints a picture on what has been published including the current knowledge and theoretical review in regards to cybersecurity and e-learning. The study endeavors to give a global picture, in Africa and narrow down to Kenya. It encompasses review of relevant materials to narrow down the established gap that the study endeavors to fulfill.

2.1 Overview of e-learning

E-learning is the term used to describe the use of platforms that utilizes internet to provide teaching and class experience to learners who are based in diversified geographical areas. The eLearning systems are dependent on the stability of the networks they ride on and the internet. According to oxford dictionary, elearning is the system that utilizes internet to provide virtual classes to learners in varied places.

Moore, Dickson-Deane & Galyen (2011), described e-learning as set of applications that have processes which delivers learning environment at any time via internet and other electronic media which includes computers and laptops among other devices, that can provide virtual classrooms and digital collaboration.

Rabai and Rjaibi (2012) noted that there is advancement in elearning systems that have evolved through the past years to diverse and widespread with features that can accommodate many users at ago.

Due to wider adoption of these systems, cyber security management is key to safeguard information derived or shared within this system by individuals, institutions and organizations. As elearning systems gain popularity, there is equally urgent need to protect them from cybercriminals who are out looking for loopholes in such systems. It has been touted that internet has become an environment where criminals wage attacks on systems that ride on it. Therefore, there is need to ensure that confidentiality, integrity and availability is not compromised on these systems. The vices such as impersonation, data manipulation and alteration need to be addressed.

2.2 Cybercrime on e-learning

Purplesec, 2021 security trends report, indicates that education records globally can fetch upto $265 Million in the black market. Cyber-Crimes on e-learning platforms, occurs where malicious users exploit the weaknesses in computer software, mobile applications, and web based tools used for providing online education to cause damages or advance their malicious activities for personal gains (Kundi, Nawaz, Akhtar & MPhil, 2014). The following are cybercrimes that are prevalent on e-learning environment:

- Unauthorized Access to Information Systems (e.g., laptop, mobile phone) illegally with the intent of damaging or misusing it or manipulating the information contained in it. In the context of e-learning it is like gaining access to the system of a course instructor or administrator for damaging or misusing the course related information e.g., student's grades.
- Unauthorized copying or transmission of Data by illegal means and further disseminating it to others without the consent of the owner. In the e-learning environment is like gathering personal information or course grades of students and disseminating it on social media.
- Unauthorized use of Identity Information, which is acquiring the personal information of other users and using it for impersonation. In the context of e-learning, is the use of email/password of other students to damage their reputation in an online class.
- Interference with information systems or data with the intent of destroying the use of functionality or services provided by it. In an e-learning environment, it is like attacking the system of an instructor to disrupt a scheduled/live lecture.
- Unauthorized Interception of confidential information by unauthorized persons. In the e-learning environment is like the interception of a list of students' email addresses to whom the password to a Zoom meeting call is to be send.
- Spamming is sending unwanted, explicit or illegal messages in huge amounts. It can also send viruses or malware. In the e-learning environment is like when a student publishes derogatory comments in a chatroom to cause chaos among the other participants.
- Email Spoofing is a cybercriminal activity where an attacker creates a false email message with a forged sender address appearing to be from legit source. This is one of the tactic employed by criminals to lure unsuspecting individuals to opening emails thinking that they are from a known source. For instance in online teaching, a student can send a spoofed email to his classmate about the class cancelation, fake assignment, results etc., impersonating the course instructor.

- Malware is a software designed maliciously and propagated through internet or through digital devices like flash disks to other computers. Such software takes many forms as Viruses and worms among other illegitimate softwares. These softwares can copy users passwords, sniff through networks to get credentials used to gain access on systems and also surveil sites most frequented to get information that can aid them to access systems.

  International Journal of Education and Research (2015), states that most e-learning systems ride on internet for its Service delivery and being a multiple user faces multiple cyber-attacks
- Due to evolving cybercrime, many criminals are seeking for loopholes on institutional systems to plagiarize other people's academic works and patent them for their benefit.
- The safeguards on online platforms is essential to deter intruders who can delete or alter contents which can lead to losses.

Majority of universities using online systems for teaching have experienced various cyber threats. The attackers employ different techniques ranging from social engineering, viruses, worms and phishing methods among other techniques to wage attacks against the online platforms. Today, criminals are operating freely in the cyberspace looking for data to sale in the black market, due to its' unique landscape which lacks physical security. Institutions of learning using online platforms have been targets for their huge voluminous data generated on daily basis. Also, students using online platforms have fallen prey to attackers who pose as students, requesting for help to use the system, where they end-up getting credentials from unsuspecting students which they use perpetuate their criminal activities.

Bandara, Ioras & Maher, (2014) asserted that many vendors have developed online systems and released them to the market without putting in place stringent safeguards, thus exposing users to cyber criminals. Further, they observed that such loopholes in these systems, have enabled hackers within the institutions of learning to penetrate these systems and alter data. They posit that criminals may change record on financial status, change date stamps on students work, inflate grades for students and misinform them among other vices that can tarnish institutions' image.

Saeed, (2021) observes that threat detection on information systems is critical and must be done as a constant monitoring and evaluation procedure to check on threats that may have been detected previously and can be handled better next time through set up of measures such as firewalls and protection software.

2.3 Synopsis of cybercrime

Internet has created a new environment refereed as cyberspace, which is key to security, learners, business community and researchers. It has enabled virtual meet-ups, where exchange of data, communication and other processes take place (Ghernaouti-Helie, 2019). This new digital landscape has bred cybercrimes among other vices waged against governments, organizations, institutions and individuals. Yar & Steinmetz, (2019), defined cybercrime as unlawful acts perpetuated by individuals where they target organizational networks, computers and other digital devices to gain access for their personal gain or cause them to deny services. Mosteanu, (2020), the adoption of varied technologies that are dependent on internet has seen increase in cybercrimes across the world.

Pathak & Nanded (2016), established that ransomware was the leading cyberattack which was waged on systems like computers to deny access to services provided by demanding some payment from users before they allow provision of such services. Kayworth & Whitten (2010), noted that much funds should be dedicated by organizations and institutions towards securing their crucial technologies that enable them perform their business.

Cybersecurity Venture's 2017 report indicated that damages by ransomware were enormous with projected losses to hit USD 20 billion by 2021, which is 57 times the amount in 2015. It went ahead to state that such attacks would be occurring after every 11 seconds in 2021, up from every 40 seconds in 2016.

According to Chitrey, Singh, Bag and Singh (2012), cybercrime brings doubts to the credibility of data held in the systems, which sometimes erodes trust on Confidentiality, Integrity and Availability of such information which jeopardizes organization's and institutions image. Standard newspaper of 8th February, 2016 asserted that while cybercrime occurrence increased globally, its pervasiveness has potential to reach crisis levels in Kenya since it is renowned for its mobile phone penetration.

Global view 2020 report by Keepnet Labs, indicated that in mid-2019 data worth USD 4.1 Billions was unprotected and the losses due to leaks was about USD 3.92 million. The report projected that cybercrime in 2021 would cause damages estimated at about USD trillion worldwide. The report also pointed out that higher percentage of attacks would be meted through mails. It avered that cyber attackers would also use different appeasing techniques to circumvent firewalls and other security controls in place. It pointed to sectors in the UK that reported cybercrime activities as follows: Consultancy firms, textile industries, institutions of learning, expatriate firms and big businesses.

Kaspersky Lab, quarter report of 2017 indicated that they were over 51 million attempts of malicious activities where over 20% of these activities targeted financial sector.

Symantec, 2016 Internet security threat report, carried out by Bank of America under Merrill Lynch Global Research, claimed that cybercrime costs approximately 540 billion euros annually in the global economy and cyber criminals potentially extract a fifth of the value created by the Internet. Team VR, 2015, report on data breach investigations, indicates that cybercrimes using phishing techniques heightened with about 23% people receiving and opening phishing messages and 11% clicking on the attachments as compared to previous year (2015).

Federal Bureau Investigation (FBI), 2015 report, through Internet Crime Complaint Center (IC3) Indicates that cybercriminals targeted business transactions that regularly use platforms that ride on internet to transfer funds. It pointed out that emails used by business community were infiltrated by scammers across 79 countries which resulted to damages estimated at the cost $ 1.2 billion.

Price Water House Coopers (PwC) 2016, report on Anatomy of Social Engineering Attack; indicated that there was a 400% phishing spike targeting government units in Europe and tax payers emails accounts to steal identifications for their use to gain access into system. In Ukraine phishing attack affected over 700,000, people where it shutdown Supervisory Control and Data Acquisition (SCADA) system servers for power supply and prohibited restarting process causing total darkness.

Herley (2012), observed that cybercrime trends in Africa were reported across the nations, stating that 51% of attacks were email based with Nigeria recording about 34% of these attacks followed by other West African states like Cote d', Ivoire, Burkina Faso, Ghana and Senegal among others.

In Kenyan View, Moturi & Mwasambo (2016) indicated that cyber criminals are targeting users on e-commerce platforms since many organizations have adopted e-commerce to carry out transactions, shop at global markets with a click of a button without involving intermediaries and remit payments online without entering a bank whole.

Serianu 2017 report indicates that mobile phone operators became a prey to cybercriminals due to huge financial transactions remitted through mobile phones and the increased betting platforms on mobile phones. The report also pointed out that Government systems were targeted by cybercriminals to cause them deny services to users; citing an illegal payment that was done in an Integrated Financial Management Information system (IFMIS) which is government managed by hackers. From the reviewed literature, cybercrime is a security concern and which is causing financial losses besides other damages. Keepnet Labs 2020 report, Education is among key sectors that have fallen prey to cybercrime like social engineering schemes. From the relevant materials reviewed, there is little study on cybersecurity management on e-learning platforms despite it's growing popularity across the globe.

Bada, Asianzu, Lugemwa, Namataba & Milburga, (2020), pointed out that adoption of elearning platforms by many countries across the globe especially during this pandemic of covid-19 would spur education to higher levels.

2.4 Global Cybercrime Damage Costs

A 2017 Report from cybersecurity ventures prediction ransomware by 2021

Table 1: Global Cybercrime Cost

S/N	COSTS IN USD	DURATION
1.	$6 Trillion	In a year
2.	500 Billion	In a month
3.	115.4 Billion	In a week
4.	16.4 Billion	In one day
5.	684.9 Million	In one hour
6.	11.4 Million	In a minute
7.	190,000	In a second

Source: Cybersecurity Ventures, 2017

2.5 Cyber threats

The infrastructure in many universities allow many students to connect their personal devices like laptops and smart phones, etc. These devices have viruses that infect the networks and create loopholes for cybercriminals to take advantage of the vulnerability and wage attacks against the important systems of the university. It is crucial that the foreign devices introduced in the network are tested and monitored to avoid attacks resulting from such devices. Albahri, S et al, (2018), notes that technology is ever changing and platforms that use internet are launched on daily basis. Some of these applications needs to be upgraded frequently from the internet, which calls for stringent measures to be put in place to ensure that hackers do not compromise such systems.

Majority of the organizations and institutions carry out penetration testing, vulnerability assessment and audit to gauge the security of their systems concerning cyber-crimes. Many institutions of higher learning are still at inception in matters related to cybersecurity initiatives (Coffey, Haveard & Golding, 2018). The upsurge reliance in e-learning platforms has provided a competitive environment for learners to achieve their dreams without being physical in a classroom(Abdullah, Toycan & Anwar, 2017). Ulven and Wange en (2021) observes that there should be response mechanism in place for institutions to mitigate any cyber threats by initiating backups immediately they sense athreat.

Cybercrimes are on the increase in institutions due to the following issues;

2.5.1 Viruses and Social Media

Imgraben & Choo (2014) posits that universities are the heavy users of social media where they can easily share their credentials without knowing. They noted it is difficult to address security issues emanating from a large population with devices hooked up on university network, adding that it is prudent for quick identification of infected devices to minimize cyberattacks. Purplesec trends report (2021), indicates that cybercriminals intruded into yahoo accounts of 3 billion people in 2013 and accessed private information.

2.5.2 Virtualization of servers

Many institutions to minimize resources, enhance performance and service delivery have embraced virtualization. Notably, devices hooked up in the virtualized environments in the event of cyber-attacks pose same threats like a desktop connected to the server, which affects also the Server.

2.5.3 Consumerization of IT

Harris, Ives & Junglas (2012) IT consumerization brings many security challenges when it comes to management of such devices in the university network. This concept has compounded the fight against cyber-threats across the globe especially in organizations and institutions of higher learning. They note that many students across the globe have embraced this concept, which has seen the rise in cyber- attacks to unprecedented levels. They further averred that technocrats and Cyber Security teams are seeking for solutions to address the challenges posed. The concepts has enabled cybercriminals scavenge for credentials through pretense by posing as authorized users to gain access to the network to advance their criminals acts.

2.6 Risk management

Patel and Zaveri, (2010), posits that it is necessary to control hazards that contribute risks, this enables one to prepare for types of risks expected and the mitigation strategies. Higher institutions of learning using e-learning platforms need to conduct assessment on risks that such platforms portends. So far, no literature is available on features in e-learning systems that can help flag out any risks related to cyber threats. Research shows that many organizations and institutions are at toddler stages and are yet to mature their cyber security functions. In most cases cybersecurity issues, have been assigned to IT administrators as one of their secondary roles (Coffey, Haveard & Golding, 2018). Cyber-security functions are key and need the involvement of all stakeholders in understanding risks and supporting the development of relevant policies (Sadok & Bednar, 2016). Many institutions perceive risk analysis as complex, requiring special expertise, thus such services are outsourced functions (Fischhoff, B. 1995).

2.7 Vendor management

Serianu, (2017) indicated that many incidents of cyber-attacks are vendor related. Negligence on part of users due to lack of enlightenment by vendors on the use of systems results to human errors that can be exploited by criminals (Banham, 2017). Due to low bandwidth in the Country most of the Universities in the Country are unable to embrace e-learning fully using their in house servers due to low internet speeds (Kashorda and Waema, 2014).

To forestall low internet speeds, the kenyan government developed an infrastructure managed under the umbrella named the Kenya Education Network Trust (KENET) to promote and foster information technology for research and teaching purposes in higher institutions. The main aim of the umbrella was to ensure that institutions get access to higher speed internet services at affordable costs (Kashorda and Waema, 2014). However, it is evident that KENET infrastructure is controlled by different entities, hence the concerns that e-learning contents could be exposed. Purplesec, 2021 security trend report, depicts that third party mistakes account to 41% cyber security breaches globally.

2.8 Training and awareness

Organizations & institutions need to create awareness programs to users of such platforms. Many institutions do not invest in security of their systems since they believe that they cannot be targeted by criminals and security is just but a technical expensive venture (Topping, 2017). Many institutions despite the rising incidents of social engineering attacks have fronted the intervening arguments. However, not all organizations have invested in cybersecurity training (Coffey, Haveard & Golding, 2018). Due to the rise in cyber threat activities, organizations and institutions need to educate users on cybercrime awareness to reduce exposure on users (Omolohunnu, 2019).

2.9 Security policies

Like financial resources, information assets need protection by the defined security policies and procedures. Likewise, institutions using e learning need to implement security policies to avoid jeopardizing their entire business (Almeidar, Carvallo & Cruz, 2018). The security policies should ensure proactive identification of Cybercrime attacks and seek ways to stop it from occurring. Many institutions give users rights to bring their own devices and connect to network (Coffey, Haveard & Golding, 2018). Institutions of higher learning need to develop procedures on the utilization of Bring Your Own Devices concept to avert attacks and guarantee a secure environment, despite the damage costs incurred by institutions emanating from such devices.

According to purplesec, the 2021 security trends report, pointed out that 64% of the education sector globally hold that their infrastructures have no protection capabilities against cyber-attacks in the next coming two years. Ford (2016) posits that protection is imperative in building digital trust by users.

2.10 Mitigation strategies of Cyber Crime

UN report of 2013 on cyber security indicated that institutions and organizations need to put in place mitigation measures through various strategies to address cyber threats. Some of strategies proposed are;

i. Enacting laws to enable investigative arm to have muscle to nail the culprits using evidence gathered electronically.

ii. Informed leadership on cybersecurity issues for easy decision making to combat threats in institutions or organizations.

iii. Campaigns through forums to create awareness on cybercrime.

iv. Multipronged approach through collaboration with various stakeholders to identify cybercriminals.

v. Technological approach both physical and logical to stop attacks.

vi. Developing cybersecurity framework to manage cybersecurity postures on e-learning platforms

2.11 Theoretical frameworks on cyber risks management

The study examined the following academic and technical theoretical frameworks to anchor the study:

Socio-Technical Systems Theory

This theory is defined on the basis that an organization consists of interacting subsystem that include people, the technical system and the internal and external environment (Pasmore, 1988). Meaning, an equilibrium in the interaction of the subsystems, is important if the organization is to effectively achieve its mission.

The theory further posits that for system change, modification or enhancement to be successful a holistic approach of the interdependent subsystems has to be undertaken. Organizational or management change fails when one aspect of the system, commonly technology is changed, and fail to analyze the impact on the interdependencies (Bostrom and Heinen, 1977).

Socio-technology theory traces its history to the coalmines in the United Kingdom in the 1940's, where new machinery was introduced into the mining system with little or no consideration on the social impact (van Eijnatten, 1997). The theory has since evolved from the two dimensional application of heavy machinery, to a holistic point of view of the modern day workplace, taking into account the social as well as technological aspects of work life. The Socio-technology principles are applied to guide system designers on the potential roles of end-users, and on understanding how new technology may be used and integrated with existing such as the case in e-learning platforms integrating with in-person learning model.

From a contextual point-of-view the socio-technology approach is being applied within the IT community (Eason, 2008), this as the demands for big tech firms to be conscious, responsible and ethical to consumers of their services, to ensure that they are not just a means to the profit-making ends (Casadesus-Masanell & Ricart, 2009).

In their seminal works, (Kline & Rosenberg, 1986) posit that it is a fallacy for one to hold that modernization is a uniform entity that resolve all issues facing the economy at a given instant, arguing that innovation fit for enhancement is based on context and need.

In August 2002, Moodle Learning Management System (LMS) version.1 was released at Curtin University, with a focus on offering a basic collaborative, construction of content platform for technical users, with no intention to scale commercially: In 19 years the basic and structurally unsound Moodle LMS has morphed into a fully functional e-learning platform that is augmented for all levels of users including features like enhancement plugins, secure logins, responsive calendar and gradebooks among others offering a rich e-learning ecosystem. The Moodle e-learning platform, is currently used to facilitate e-learning in the three universities researched in this study.

The Covid-19 pandemic has had far reaching ramification on every aspect of life, including working and learning away from a designated physical location, which has vividly supported the notion that firms needed to be adaptive both internally and externally to change (Dreyer & Gronhaug, 2004). The relevance of the socio-technology theory to institutions of learning like universities, vis-à-vis this research, therefore is in underlying capability to explain the nature of management of information systems, to deliver on its core technical functionality while addressing the social (users) needs. For instance, e-learning platform Moodle, to cater for the need of the users for a user friendly, tailor-made experience while remaining secure, responsive and commercially viable. This requires a clear structure to address issues like the user experience while taking into account key technology features like online security or data privacy.

Task-Technology Fit (TTF) theory

Theory is said to be one of the most fundamental components or elements of research (Creswell, 2014; Lim, Saldanha, Maliadi & Melville, 2013). Goodhue & Thompson, (1995) explains the use of technology by examining the fit of technology to task and requirements. The theory seeks to add knowledge on technology utilization in management of public and private entities.

TTF is the predominant theory that explores the post-adoption characteristics of technology use (Goodhue & Thompson, 1995). Other theories, for instance the diffusion of innovation theory consider the antecedent factors that inform the adoption and use of technologies. Task-technology fit theory examines the characteristic of the interdependence of the persons (a user), technology (the software, hardware and/or information ecosystem) and the task (assignment or objective set out to be accomplished by the user of the technology). Moreover, the theory tests the assumption that the utilization of information systems results in improved output only on condition that technology purpose corresponds to users' task requirements (Ching Lin Huang, 2008). The TTF approach propose three subsets in the understanding of the post-adoption use and effectiveness of technology.

The first considers the users, by determining a combination of the task objective and features of the technology toward achieving the task objectives (Rai and Selnes, 2019). The degree to which a technological system facilitates an individual in performing his or her tasks is measured by the user grading the system based on the following indicators: quality, deploy-ability, compatibility, security or authorization levels, timeliness, reliability, ease of use and access with and between users.

The second subset evaluates the task characteristics. The technology characteristics are the technology-specific attributes or functions. This second proposition of the TTF theory posits that the use of technology, in this case ICT tools, by individuals is dependent on the perceived fit. ICT tools refer to hardware and software technologies. The level to which the technology facilitates the efficient meeting of set objectives while requiring minimal resource investment or allocation by the user(s). And while hardware devices continue to refine their offering to meet customer and market demands, the number of software system or information systems have also increased greatly including administrative, human resource management, enterprise resource planning, cybersecurity management systems among others (Quintaine, et.al., 2011). The application and perceived efficiency of the ICT tool fundamentally determine the choice and utilization.

The third subset of the theory hypothesizes that a positive evaluation of task-technology fit not only predicts use, but positively influences perceived outcome (Goodhue & Thompson, 1995). It aims to understand what aspects contribute to the perception of higher performance, "based on the capabilities, a technology extends its services to perform particulars tasks for a user" (Tripathi and Jigeesh, 2015).

The relevance of the theory, TTF provides an empirical basis to investigate the fit of technology available cyber security ICT tools being applied in the institutions of higher learning in this study. The role of technology is now an indispensable part of education, learning and teaching process. The Task-Technology fit is the degree to which the applied technology in this case ICT cybersecurity modules assist the organization achieve the set portfolio of tasks the technologies are designed to perform, evaluated based on IT professionals' assessment and end user perception.

Organizational information processing theory (OIPT)

OIPT conceptualizes the gap between contextual factors and management policy and practice, as the missing link between internal and external factors (Tushman & Nadler, 1978). The unit of analysis is the organization, including internal units of business or operational processes.

Organizational processes are diverse mainly ranging from automated, to knowledge based and creativity related processes, each with diverse characteristics and uncertainties (Feitzinger and Lee, 1997). Organizations attempt to manage the inherent transient uncertainties of this diverse process, by putting in place tools for coordination and control like rules and defined procedures, hierarchy, and information systems.

OIPT posits in considering management policy or practice the diversity of the process characteristics is fundamental in ensuring efficiency in an organization as a whole (Daft and Lengel, 1986). Meaning, the theory is applied by researchers to determine what influences an entity's, information-processing framework. Organizations are information processing systems that are constantly dealing with uncertainty for instance, and relevant to this study, cyber security threats.

The organization information processing theory is applicable to this study, as we are able to explain the need for cybersecurity management on e-learning systems in institutions of higher learning. Cybersecurity is a key process within the information system, with specific task objectives as well as various inherent uncertainties: The former including variables like identity verification, data privacy, responsiveness while the latter including the users' compliance and skills. The theory explains that management of the e-learning platforms need to develop policy that facilitates effective coordination between the information system needs and information processing requirements to sufficiently meet the overall objectives, i.e., facilitate an effective online experience.

The COBIT framework

This framework defines processes in the business environment and how technology can be controlled to achieve the objectives. It has varied measures that are well structured and when utilized it yields coherent processes for IT (Haes & Grembergen, 2020). The framework permits distinct procedures aimed at imparting finest practices in the management of information technology within the establishments. The framework also underscores the need for users to comply with rules set to support configuration & execution of ICT authority and regulatory framework (ISACA, 2018). However, this framework depends also on user skills which does not guarantee management of cybersecurity on e-learning platforms.

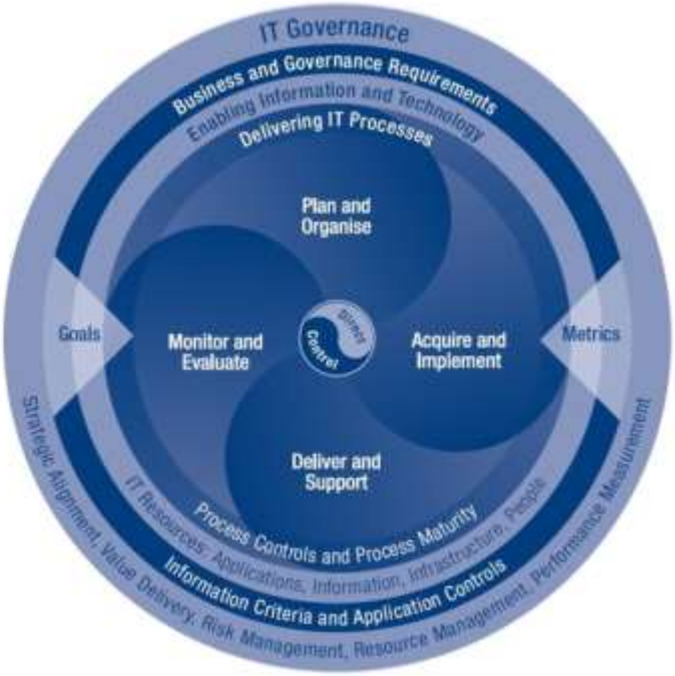

IT Governance
Business and Governance Requirements
Enabling Information and Technology
Delivering IT Processes
Plan and Organise
Goals
Monitor and Evaluate
Direct
Control
Acquire and Implement
Metrics
Deliver and Support
Process Controls and Process Maturity
IT Resources: Applications, Information, Infrastructure, People
Information Criteria and Application Controls
Strategic Alignment, Value Delivery, Risk Management, Resource Management, Performance Measurement

FIGURE 1. COBIT FRAMEWORK

Source: COBIT following are **4.1 Framework for IT Governance and Control (ISACA)**

Domains covered in this framework are:

Plan & organize: - Structuring of systems and planning them to realize goals and objectives of the business.

Acquire & implement – Getting the right technologies and rolling them out in the institutions. **Delivery & Support**: - This leverages on supervision to ensure provision of services.

Monitor and Evaluate: - Assessing results through feedbacks in accordance to the requirements to see whether the system is still worthwhile its course or need some adjustments.

The National Institute of Standards and Technology (NIST) Framework

It provides guidelines to evaluate and modify processes for better results in the organizations to foil any cyber threats. It makes organizations and institutions to be proactive in risks management.

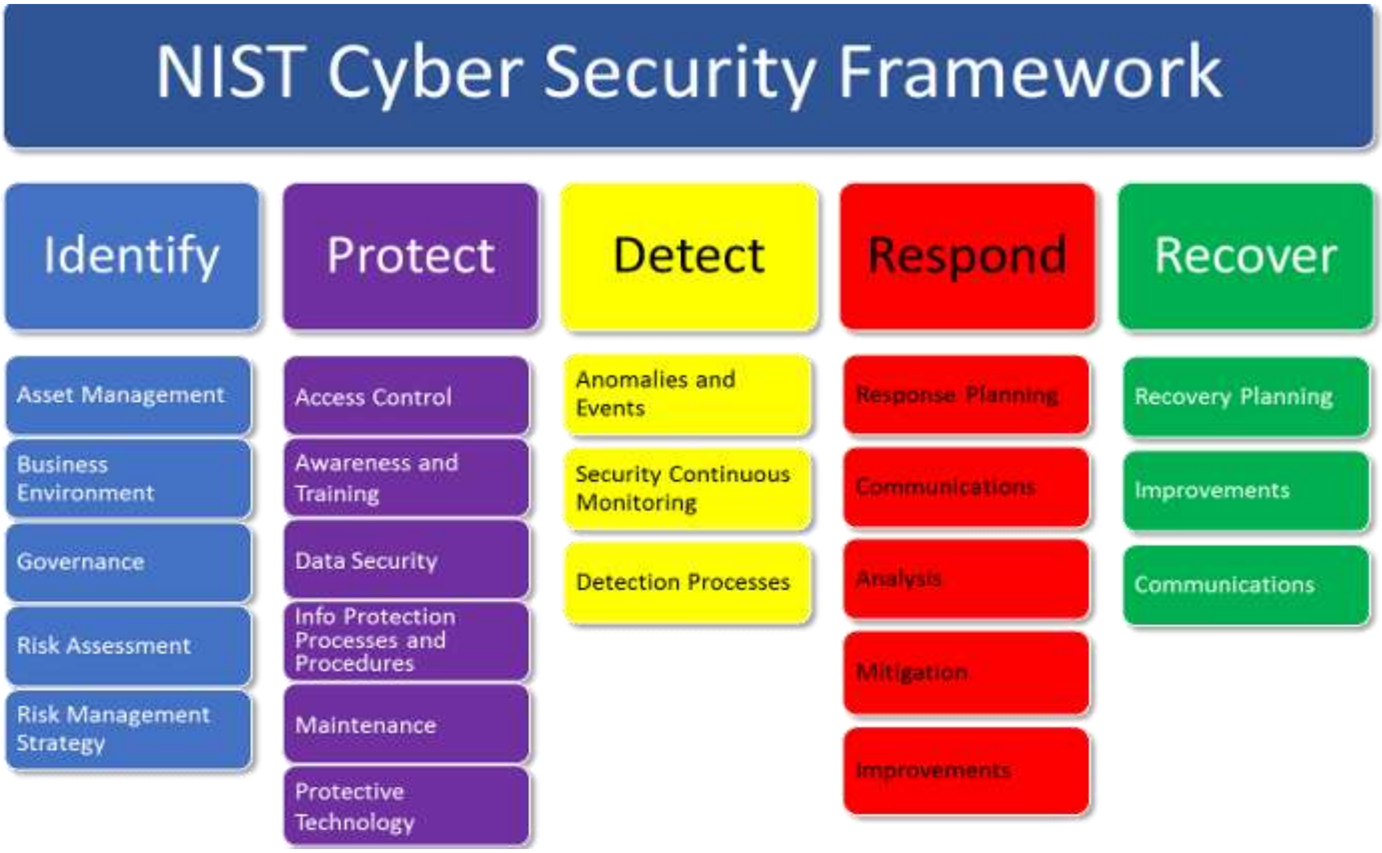


FIGURE 2: NIST CYBERSECURITY FRAMEWORK

Source: Introduction to the NIST cybersecurity framework for landscape of menaces (Paganini, 2017)

This framework has five modules;

Identify: It puts measures in place to handle any cyber risks that may hamper the management of operations.

Protect: Putting measures in place with proper controls that fosters conducive environment which guarantees key Service delivery.

Detect: This documents procedures that help to point and flag out any anomalies identified in the system to minimize damages and reduce delay time.

Respond: It activates corrective measures on the anomalies detected to ensure that the error is eliminated appropriately.

Recovery: Remedies to ensure continuity by providing resilient fallback and rescue plans.

ISO 27001/27002

These are Organization for Standardization (ISO) published information security standards named ISO 27001/27002. They are used in complementary to limit any errors or threats. ISO 27002 has varied features that interlink with features in ISO 27001 to provide a robust standard with documented procedures for best management practices. These standards provide guidance for enhancing security on existing systems with ultimate aim of securing business assets.

The procedures include six steps.

1. Description of rules
2. Defining the boundaries
3. Assess hazards
4. Control hazards recognized
5. Weighing checks to be effected
6. Documenting Standard operation procedures.

2.12 Gaps in the reviewed frameworks

The review of various scholarly sources on the various frameworks identified the following gap; the existing frameworks reviewed places prominence on fears and exposures on organizational systems, inadequate framework to manage cybersecurity on online learning systems. The study attempts to narrow the knowledge gap through proposed effective framework with features borrowed from K-12 Cyber protection Framework.

K-12 Cyber Protection Framework (CPF)

It focuses on setting standard best practices on cyber security, cyber safety & privacy on institutions. It stands on other frameworks tailored for securing businesses assets from cyber-attacks like COBIT-5 and NIST. It also borrows heavily from these frameworks due to their tested features that have been adopted and modified to suit different environments. K-12 CPF has preference compared to other frameworks since it provides common knowledge or language that is simple for many institutions to understand, manage, and express cybersecurity risks. It is quite adaptable and can be utilized uniformly by many institutions. In other words, it has features that easily fits and suits the institutional needs.

See Figure 3 below.

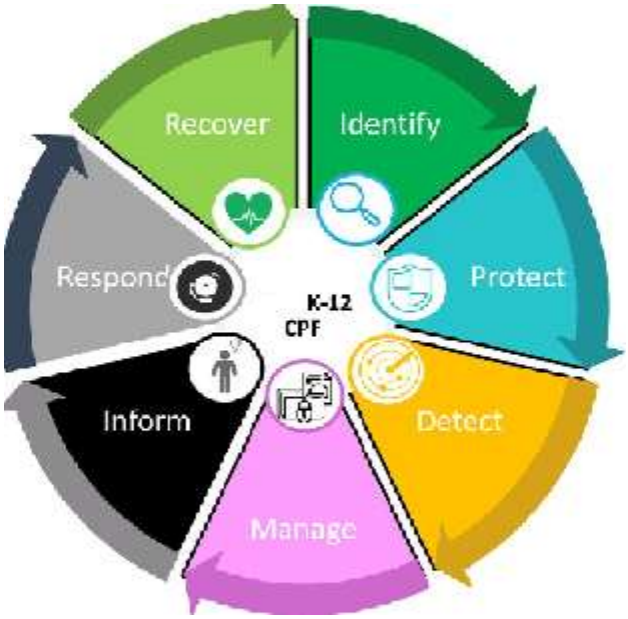


Figure 3: **The K-12 Cyber protection Framework**

Source: K-12 Cyber protection Framework (Kamaludeen, Ismaeel, Asiri, Allen & Scarfo, 2020)

K-12 CPF modules:

The **identify** module of the framework focuses on developing an official compassion on management of cybersecurity on e-learning platforms within the learning institutions. Categories of identify function are as follows:

1. Asset Management: This is the aspect that controls institutional assets to ensure that the objectives are achieved by minimizing risks.
2. Business Environment: It fosters conducive environment that enables institutions to thrive well and achieve their missions and operate optimally in a competitive manner.
3. Governance: For seamless information flow and to foster communication regarding cybersecurity issues to ensure best practices are adhered to.
4. Risk Assessment: Evaluate hazards posed by cybercrime on institutions’ functions, mission, image, or reputation for individuals and/or assets.

5. Risk Management Strategy: Ensuring that there is a fallback plan to address and mitigate risks when they occur.

The **Protect** module of the framework ensures that the defense mechanisms is in place. The category of this function includes:

1. Putting in place both physical and logical barriers to ensure that the assets are protected.
2. The University should conduct in-house training and create cybersecurity awareness programs to reduce cyber threats as users have been deemed to be the weakest link.
3. Protecting data asset to guarantee data integrity, availability and reliability.
4. Putting polices in place to address security issues, procedures, process and management of e-learning platforms.
5. Maintenance and signing of Service level Agreements (SLAs) to ensure that there is no delays when the system malfunctions.
6. Cyber-safety to ensure that the users of the system are secure and their privacy rights are not violated by sourcing robust systems and installing them to guarantee consistency.

The **Detection** module involves identifying cybersecurity event occurrence through developing and implementing appropriate activities. The function includes:

1. Anomalies and Events: Detecting anomalous activity and understanding the potential impact of events on e-learning platforms.
2. Continuous Security Monitoring: Identifying cybersecurity events and verifying the effectiveness of protective measures within e-learning platforms.
3. Detect Processes: maintaining and testing detection procedures and processes to ensure awareness of anomalous cyber-safety and cybersecurity events within e-learning platforms in public universities.

The **Inform** module involves developing and implementing appropriate activities to have a credible understanding of e-learning platform systems. The function includes:

1. Transparency Processes and Procedures: Maintaining and using policies, processes, and procedures to growth the transparency of the University e-learning practices.
2. Privacy and Safety Awareness: The Universities should create and promote awareness on privacy and safety protection practices. By maintaining and using procedures and processes to increase

predictability consistent with the Universities strategy to protect students' and educators' privacy and safety in e-learning platforms.

The **Respond** module involves developing and implementing suitable activities by Universities to response a detected cybersecurity incident. It supports the ability to contain the impact of a potential cybersecurity incident. The function includes:

1. Response Planning: Procedures and processes implemented and maintained as a response when cybersecurity incidents are detected on e-learning platforms.
2. Communications: Coordinating response activities with internal and external support and stakeholders (law enforcement agencies an example of external support).
3. Analysis: Detailed examination of responses and recovery support activities to ensure the effectiveness of processes and procedures used within e-learning systems.
4. Mitigation: Performing activities to prevent the expansion of events through mitigation of the effects to resolve the incident within e-learning systems.
5. Improvements: University response and detection to current and previous activities can be improved by using lessons learned from previous activities within e-learning platforms.

The **Recovery** module involves maintaining plans for resilience and restoring capabilities and/or services that were affected due to a cybersecurity incident through developing and implementing appropriate activities within e-learning environment. It's functions includes:

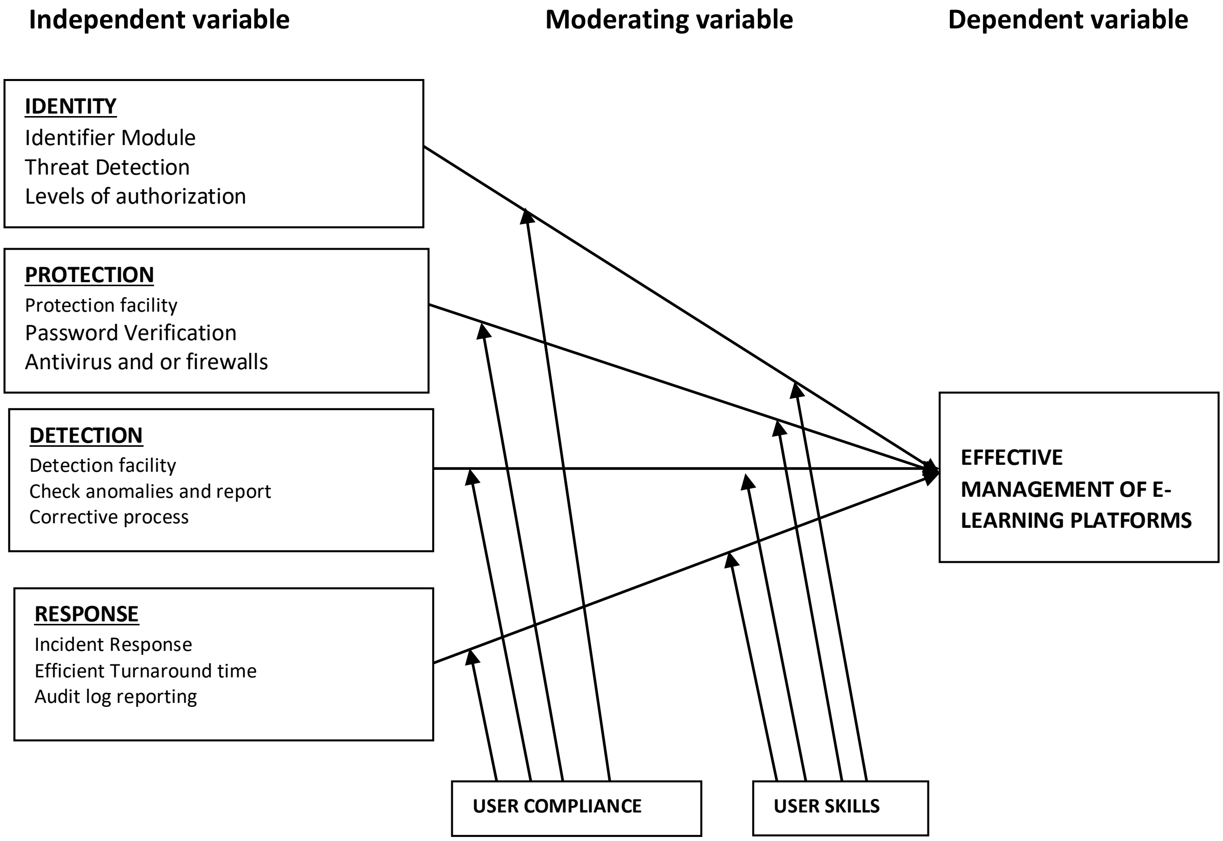
1. Recovery Planning: Executing and maintaining procedures and processes to keep the restoration/recovery of e-learning systems affected by cybersecurity incidents within the public universities.
2. Improvements: Improving recovery processes and planning by incorporating lessons learned into future activities.
3. Communications: Coordinating Universities with other parties (internal and/or external), e.g. ISPs, victims and vendors, etc.

2.13 Conceptual framework

The framework borrows heavily from K-12 Cyber Protection Framework (CPF), which is anchored on top of other frameworks that guarantee management of security issues on online platforms. It consists of features which are critical in addressing management and control of cybersecurity on eLearning platforms in institutions of learning.

The variables are derived from K-12 CPF security features adopted from other frameworks reviewed in the study which includes; ISO27002, CIS, NIST and COBIT 5. It has incorporated the intervening variables namely user compliance and user skills in the framework to increase accuracy during assessment of e-learning platforms. User compliance and User skills may have direct influence on cybersecurity when it comes to identity, protection, detection and responding to cyber threats. These variables provide an impetus to address the management of cybersecurity on e-learning platforms in public universities.

Figure **4. CONCEPTUAL FRAMEWORK**



Source: Author

Study Proposition

This study examined the following hypothesis:

HO_1: There is no substantial effect of identity on effective management of cybersecurity on e-learning platforms in Public Universities in Kenya

HO_2: There is no weighty effect of protection on effective management of cybersecurity on e-learning platforms in Public Universities in Kenya

HO_3: There is no significant effect of detection on effective management of cybersecurity on e-learning platforms in Public Universities in Kenya

HO_4: There is no major effect of response on effective management of cybersecurity on e-learning platforms in Public Universities in Kenya

HO_5: There is no statistically significant relationship between user compliance and identity on effective management of cybersecurity on e-learning platforms in Public Universities in Kenya

HO_6: There is no statistically significant relationship between user compliance and protection on effective management of cybersecurity on e-learning platforms in Public Universities in Kenya

HO_7: There is no statistically important relationship between user compliance and detection on effective management of cybersecurity on e-learning platforms in Public Universities in Kenya

HO_8: There is no statistically significant relationship between user compliance and response on effective management of cybersecurity on e-learning platforms in Public Universities in Kenya

HO_9: There is no statistically significant relationship between user skills and identity on effective management of cybersecurity on e-learning platforms in Public Universities in Kenya

HO_{10}: There is no statistically significant relationship between user skills and protection on effective management of cybersecurity on e-learning platforms in Public Universities in Kenya

HO_{11}: There is no statistically significant relationship between user skills and detection on effective management of cybersecurity on e-learning platforms in Public Universities in Kenya

HO_{12}: There is no statistically significant relationship between user skills and response on effective management of cybersecurity on e-learning platforms in Public Universities in Kenya

2.14 Operationalization of Variables

Table2: Operationalization of variables

Variables		**Roles**	**Indicators**	**Units of measure**
Independent Variables	***Identify***	• *Inbuilt facility to identify threats*	• *Identifier Module* • *Threat Detection* • *Levels of authorization*	• *Effectiveness on scale (1to5)*
	Protection	• *Inbuilt facility to protect threats*	• *Protection facility* • *Password verification* • *Antivirus or firewalls*	• *Effectiveness on scale (1to5)*
	Detection	• *Facility to detect threats*	• *Anomalies & Events* • *Continuous security monitoring* • *Corrective process*	• *Effectiveness on scale (1to5)*
	Response	• *Facility to respond to threats*	• *Incident response* • *Recovery Planning* • *Audit log reporting(inform)*	• *Effectiveness on scale (1to5)*
Dependent variable	***E-learning platforms***	• *Effectiveness of cybersecurity management on e-learning platforms*	• *Support from the independent variables*	• *The perceived links of the independent variables scale (1to5)*

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter highlights step-by-step approach adopted for the study. It shows how designs were established, population of the study, sample of the population, sampling procedures employed, tools used, how data was gathered, instruments testing for reliability and processing of data to determine the variables.

3.2 Research Design

The enquiry was carried out in three Kenyan public universities, to establish how cybersecurity was being managed on e-learning environment. The focus of the study was on management, operational and controls involved. This study espoused the logical philosophy that supports the use of varied approaches in examination of variables under study with concentration on the reality regarding the research questions under investigation. Using this approach, whichever procedures, practices and processes associated with quantitative or qualitative research were utilized. It takes cognizance that every technique has its limitations and different approaches, thus necessary to complement each other.

Quantitative approach emphasizes measurement and data analyzed in a numerical form to give precise description. According to Mugenda and Mugenda (2003), quantitative approach also known as the scientific method was considered as the traditional mode of inquiry in both research and evaluation. Quantitative approach places emphasis on methodology, procedure and statistical measures to make predictions. According to Berg (2001), qualitative research helps in analyzing information in a systematic way by use of common words or phrases in order to come up with useful conclusions and recommendations on the social settings and the individuals who portray those characteristics. This research was a case study of three selected public universities using e-learning platforms.

3.3 Target Population of the study

Zikmund, Babin, Carr and Griffin (2013), define population as the large collection of all subjects from which a sample is drawn. Kombo and Tromp (2009) defined the target population as a group of individuals, objects or items from which samples are taken for measurement. It is the population to which a researcher wishes to generalize the results of their study (Mugenda & Mugenda 2012). Therefore, the study population comprised of the public chartered Universities in Kenya as per the Commission for University Education (CUE) 2017/2018 University Statistics report. See Appendix1. Due to constraints, only the three Public Chartered Universities were purposively selected for the study. The selection criteria was based on the following; size of the public university, and geographical location of the University in Kenya mapping out the regions in the Country, and must be currently using e-learning platforms. Therefore, the study identified 3 universities; one based in Central and/or Eastern Kenya (University A), one based in the Coastal and/or Nairobi hubs (University B) and another university based in Rift Valley and/or Western Kenya (University C) which constituted the target population for the study.

3.4 Sample Size and Sampling procedure

This study adopted a multi-stage sampling procedure. Stage one involved an evaluation to establish the prevalent e-learning platforms used at the three universities, which according to a report by The Electronic Journal for E-learning (EJEL) and International Journal of E-Learning and Distance Education (IJEDE) are; Google Class, Zoom for Education and Moodle.

Stage two involved purposive sampling and selection of two schools or faculties from each university that were offering common undergraduate degree programs using e-learning platforms namely; the Bachelor of Computer Science or Business Information Technology, Bachelor of Commerce (B. Com) or Business Administration and Bachelor of Science in Electrical engineering or Electronics &Telecommunication.

Stage three involved the selection of departments from each faculty/school for inclusion in the study. Purposive sampling was applied in the selection of one department in each of the identified two-degree programs in three universities. Only departments that had more than 20 lecturers and over 180 students using e-learning platforms were included in the sampling process. Two departments per university were selected, giving six (6) departments from the three universities.

Stage four involved selection of lecturers and students who were the main respondents of this study. From each department, six (6) lecturers were randomly selected. The two departments sampled from each university gave thirty-six (36) lecturers, which formed the sample size from the three public universities. From the student population, ten (10) students per department were randomly selected, giving twenty (20) students from two departments per university. This resulted in a total sample of sixty (60) students from the three universities.

Stage five involved purposive sampling and selection of six (6) administrators from e-learning staff or ICT administrators from each university, which gave eighteen (18) administrators. This aided in assessing management of cybersecurity on e-learning platforms. Illustration of the respondents is as in the table below

Total number of respondents in selected public universities

Table3: Sample Size

S/N	Respondents	per university		For three universities
1.	Students	20	20*3	60
2.	Lecturers	12	12*3	36
3.	Elearning staff/Administrators	6	6*3	18
4.	**Total sample size for three universities**			114

3.5 Data Collection Instruments

Primary data and secondary data were used. A structured questionnaire was used for the collection of primary data. In each of the selected university, a contact person assisted in administration of questionnaires. The questionnaires comprised of Likert scale that was developed to capture the various variables under study. A questionnaire is a research instrument that gathers data over a large sample and its objective is to translate the research objectives into specific questions and answers for each question to provide data for hypothesis testing (Mugenda & Mugenda, 2003). The questionnaire sought to determine respondents' opinions on the management of cybersecurity on e-learning platforms in public university.

The questionnaire was divided into two sections, for closed and Likert scale questions. The first section was obtained from survey data collected from the three Universities to determine the state of cybersecurity management on e-learning platforms. The data relevant to the conceptual framework of the study was selected for analysis. The second section-involved use of likert scale to collect qualitative data based on the conceptual framework. See appendix 4 for questionnaires.

For Secondary data, a review of existing documents was done during literature review. Documents sourced from online journals, international publications and internet data were used to gather data on cybersecurity management frameworks.

In carrying out cybersecurity assessment on e-learning platforms the following steps were used based on the conceptual framework;

1. **Prioritization and scope definition**: To obtain an understanding of the current approach to governance and management of cybersecurity on e-learning platforms in the selected three Public Universities.

2. **Assessment and profile creation**: To gain an understanding of the e-learning systems at the three universities and assessment of assets that enable the mission described in Step 1. It involves also identifying of threats and vulnerabilities on e-learning systems and assets.

3. **Risk assessment and creation of target profile:** involves analysis of the operational environment and overall risk management practices besides understanding the current state and defining target cybersecurity posture of the e-learning platforms.

4. **Gap prioritization:** It encampasses documenting the actions required to close the gaps between current and target state environments, through recording the differences between the two profiles.

5. **Action Plan and Cycle Management:** After the gaps are known and the plans have been determined to close those gaps, the universities can execute the plan that addresses their priorities to improve security and meet their cybersecurity management goals on e-learning platforms. Then provide ongoing review/assessment of the overall success of the initiative, identify further governance and management requirements to support continuous improvements.

3.6 Data Collection Procedure

Data collection is the gathering of information to serve or prove some facts (Kombo & Tromp, 2009). Questionnaire were self-administered to the respondents and three research assistants were recruited and trained for quality results to be achieved. Secondary data was collected from published sources such as library, internet and research done by other scholars. The target participants were students, lecturers using e-learning, and staff who manage the e-learning platforms. The e-learning management staff were key as they are deemed knowledgeable on utilization of e-learning systems as end users. The universities under study were contacted by use of introductory letter from the School of Computing and Informatics, where research assistants/contact person introduced their intents besides issuing questionnaires to respondents and waiting for feedback.

3.7 Validity and Reliability

Mugenda and Mugenda (2003) noted that validity should reflect what is in the collected data and after analysis and give a picture representing the environment under study.
This study adopted content validity where the domain of the concept was made clear and the analyst judges opine whether the measures fully represent the domain (Bollen, 1989). Drost (2012) posits that there are two ways of assessing content validity, that is, by asking a number of questions about the instrument or test and/or asking the opinion of expert judges in the field. Content validity was tested by formulating questionnaire and operationalizing it as per the study variables. This ensured adequacy and representativeness of the items in each variable in relation to the purpose and objectives of the study.

The study used Cronbach's alpha to test the reliability of the items. Reliability was achieved through the test-retest reliability method using the Cronbach's Alpha (α) in SPSS statistics. The same questionnaire was administered to a sample of 10 respondents in university A. The first test was done during the pilot testing stage followed by two other subsequent tests to the same group of respondents at an interval of three weeks. Data from the Likert scale for questions under each construct was then analyzed to generate the Cronbach's alpha coefficient. According to (Namdeo & Rout, 2016) Cronbach measures test scores from a range of zero to one scores closer to one indicate high reliability more over test scores above 0.6 are sufficient for study. The overall reliability of the test score was measured in Table 3.1 with a score of 0.742 indicative of the suitability in the study. Table 3.2 indicates that the items were all above 0.6 therefore indicating the questionnaires fit in the study.

CRONBACH’S RELIABILITY STATISTICS

Table4: Cronbach's Reliability

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.741	.742	15

TABLE ITEM TOTAL STATISTICS

Table5: Item Total Statistics

Item-Total Statistics

Items	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Identifier Module	63.3889	48.016	.474	.714
Threat Detection	63.3444	49.374	.436	.719
Authorization Levels	63.3333	54.764	.049	.756
Protection Facility	63.3333	53.281	.129	.750
Password Verification	63.3333	54.562	.056	.756
Antivirus Or Firewall	63.3556	47.108	.525	.708
Inbuilt Detection	63.2444	54.367	.093	.750
Anomalies And Reporting	63.2889	50.545	.313	.731
Corrective Process	63.3222	48.311	.477	.714
Incidence Response	63.3222	48.558	.454	.716
Efficient Turnaround Time	63.3333	49.843	.350	.727
Audit Log Reporting	63.4333	51.484	.263	.736
Skills	63.1778	48.305	.568	.708
User Compliance	63.3444	48.138	.522	.710
Management of E-learning Platform	63.4222	47.438	.492	.711

Source: Research Data (2021)

3.8 Data Analysis and Presentation

Zikmund et al. (2012) posit that data analysis is the application of reasoning to understand the data gathered with the aim of determining consistent patterns and summarizing the relevant details revealed in the investigation. Data processing entailed coding, analyzing, classification and tabulation of data collected so that they are amenable to analysis (Kothari, 2009). The data was analyzed using Statistical Package for Social Sciences (SPSS) version 24 guided by the research objectives and questions. Analysis involved use of descriptive and inferential statistics techniques that took care of the quantitative data gathered during the study. Descriptive statistics included standard deviations, means, frequencies and percentages while inferential statistics entailed regression analysis.

The multiple regression analysis consisted the analysis of variance (ANOVA) and regression coefficients. The multiple regressions determined the relative importance of independent variables in respect to dependent variables. Regression analysis was performed to determine the influence of the independent variables in predicting the dependent variable.

3.9 Ethical Consideration

Research purpose was clearly communicated to the respondents through questionnaires. Privacy and anonymity was assured to the respondents. In addition, Consent was sought through an introduction letter which was presented to the institutions of study and the target respondents before carrying out research.

CHAPTER FOUR

RESULTS AND DISCUSSIONS

4.1 Introduction

This chapter outlines analysis of research data, research findings and finding discussions. The findings were evaluated according to research objectives and methodology to ensure that research questions are answered. The findings contain results related to demographic characteristics, descriptive analysis and inferential statistics. The study was carried out in the three universities based on the defined criteria in the methodology where lecturers, students and e-learning administrators were requested to provide their views & perception regarding management of cyber security on e-learning platforms.

4.2 Response Rate

114 questionnaires were issued out to the target respondents in three universities. 90 questionnaires were returned back as responses, which implied 78.94% response rate, which were adequate to make recommendations and conclusion of the study. According to (Mugenda & Mugenda, 2003) a response rate of 50% is adequate for analysis reporting, a rate of 60% is good, and a rate of 70% and over is excellent. Based on this assumption, the received response was considered sufficient for analysis.

Response Rate

Table6: Response Rate

Response rate	Frequency	Percentage (%)
Returned	90	78.94
Unreturned	24	21.06
Total	**114**	**100**

Source: Research Data (2021)

4.3 Demographics

The age of the respondents was sought for

Age category

Table7: Age Category

Age Category	Frequency	Percent (%)
19-23	7	7.8
24-29	9	10.0
30-34	31	34.4
35-39	8	8.9
40-44	8	8.9
45-49	15	16.7
55 and over	12	13.3
Total	**90**	**100.0**

Source: Research Data (2021)

The study showed the ages of respondents presented in Table 7. The ages 30-34 represented 34.4 percent, 45-49 was 16.7 percent, 55 and above represented 13.3 percent, 24-29 indicated 10 percent, 35-39 and 40-44 showed 8.9 percent and between 19-23 was 7-8 percent. The results indicated there was a mixed sample of different age categories that gives a broad sample size.

POSITION OCCUPIED

Table8: Position occupied

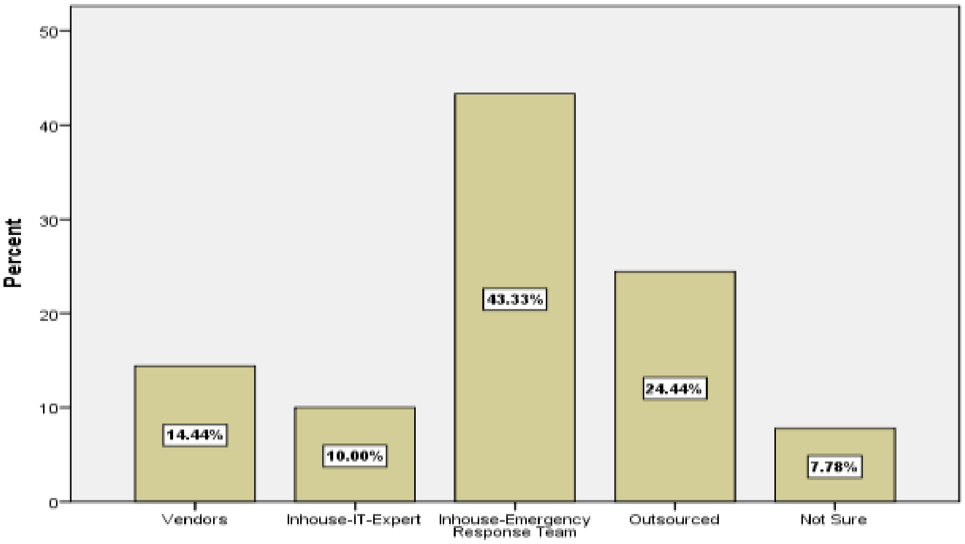
Position	Frequency	Percent (%)
Student	42	46.7
Administration	18	20.0
Lecturer	30	33.3
Total	**90**	**100.0**

Source: Research Data (2021)

4.4 Cyber Security Management

The study sought to establish how cyber security is managed within the institutions it was observed from figure5 that majority of the institutions managed cyber security through in house emergency response teams 43.33% followed by outsourcing 24.44%, vendor based at 14.44%, in house IT expert 10% and lastly 7.78% respondents were not sure how this process was carried out within the institution.

Figure 5: Cyber Security Management

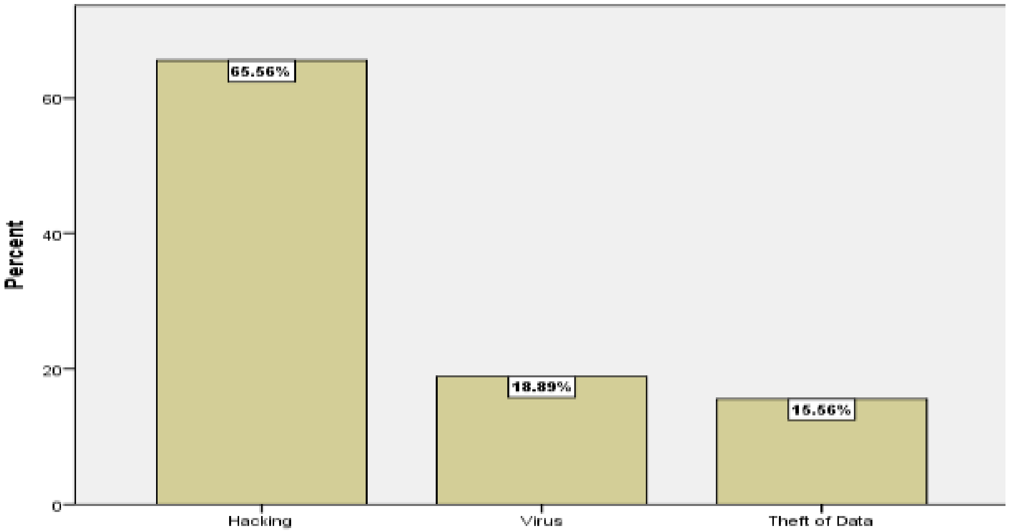


Source: Research Data(2021)

4.5 Prevalent Cybercrime

The study purposed to establish the prevalence rate of different types of cyber crimes commited within the institutions, the most prevalent crime was hacking 65.56%, followed by virus attacks 18.89% and finally theft of data was 15.56% as indicated by figure 6 below

Figure 6: Prevalent Cyber Crime

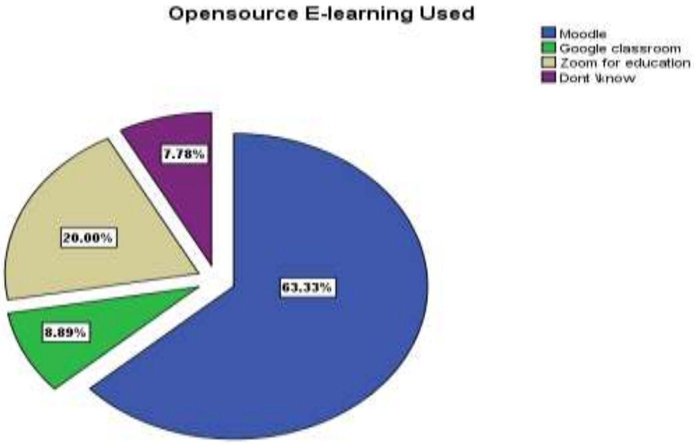


Source: Research Data (2021)

4.6 ELearning platforms

The study purposed to establish different e-platforms in use at the public universities. The use of Moodle system accounted for 63.3%, Zoom for Education 20%, Google classroom 8.9% and those who don't know the type of e-learning platform used accounted for 7.8 percent.

Figure 7: E-learning platform used in institutions



Open-source e-learning management system

Source: Research Data (2021)

4.7 Security testing

The study examined the security testing mechanisms that were available and being used in the institutions Table 9 indicates that vulnerability testing 41.1% was done constantly, followed by penetration testing 28.9%, audit controls 23.3% and lastly respondents who were not aware of any security testing mechanisms were 6.70 percent.

Table9: Security Testing

Security Testing	Frequency	Percent (%)
Vulnerability Testing	37	41.1
Penetration Testing	26	28.9
Audits	21	23.3
Don't Know	6	6.70
Total	**90**	**100.0**

Source: Research Data (2021)

4.8 Trainings and awareness

Different institutions undertake trainings and awareness, the study sought to establish the rate at which this was carried out. Table 10 indicates that weekly trainings accounted for 63.3% followed by monthly at 17.8%, never undertaken 10% and lastly yearly basis at 8.90%.

Table10: Training & Awareness

Training and Awareness	Frequency	Percent (%)
Weekly	57	63.3
Monthly	16	17.8
Yearly	8	8.90
Never	9	10.0
Total	**90**	**100.0**

Source: Research Data (2021)

4.9 Server Hosting

Table 11 indicates whether the institutions had their own servers or it was vendor based. The results indicated vendor based accounted for 54.4% and those who used own servers at 45.65 percent.

Table11: Server Hosting

Hosting	Frequency	Percent(%)
Servers	41	45.6
Vendors	49	54.4
Total	**90**	**100.0**

Source: Research Data (2021)

4.10 Descriptive analysis

Responses received were analyzed using standard deviation (Std Dev), Mean and percentages. Respondents were provided with a five point Likert scale namely Strongly Disagree (SD), Disagree (D), Neutral (N), Agree (A) and Strongly Agree (SA) from which they were required to give an opinion on effective management of cyber security on elearning platforms in their institutions. The topics of response included; Effect of identity on elearning platforms in public universities, Effect of protection on e-learning platforms in public universities, Effect of detection on e-learning platforms in public universities, Effect of response on e-learning platforms in public universities, E-Learning platforms requirements and Skills & User Compliance Requirements**.**

4.10.1 Effect of identity on e-learning platforms in public universities in Kenya

The instrument intended to establish the level of agreement and disagreement on statements about identity on elearning platforms. The results were presented in Table 12, which shows varied responses.

DESCRIPTIVE STATISTICS FOR IDENTITY REQUIREMENTS

Table12: Identity Requirements

Identity factors	**SD%**	**D%**	**N%**	**A%**	**SA%**	**Mean**	**Std Deviation**
Does the e-learning platform at your university have an identity facility	5.6	3.3	6.7	7.8	76.7	4.4667	1.1238
Does the identity facility alerts when threats occur s	4.4	3.6	2.2	16.5	73.3	4.5111	1.0194
Does the identity facility have authorization levels for the different categories of users	2.3	6.7	4.3	7.8	78.9	4.5222	1.0624
Total Averages	4.1	4.5	4.4	10.7	76.3	4.5000	1.0685

Source: Research Data (2021)

First, the study sought to establish whether the elearning platforms at the institutions had identity facility. From Table 12, the results showed that 5.6% strongly disagreed, 3.3% disagreed, 6.7% remained neutral, 7.8% agreed and 76.7% strongly agreed, giving a mean of 4.667 and standard deviation of 1.1238. The results showed that majority of the respondents agreed that the elearning platforms in their institutions had identity facility. The results further showed that the identity facility had authorization levels for different categories of users and affected the management of elearning platforms largely with a mean of 4.5222 and standard deviation 1.0624. The results also showed that the identity facility could identify threats/attackers with a mean of 4.5111 and a standard deviation of 1.0194. The entire averages of the items under identity gave a mean score of 4.5000 and standard deviation of 1.0685, which implied that identity strongly, affected effective management of elearning platforms in Public Universities.

4.10.2 Effect of protection on e-learning platforms in public universities in Kenya

The study further established effect of protection on elearning platforms. The results were presented in table 13

DESCRIPTIVE ANALYSIS FOR PROTECTION REQUIREMENTS

Table13: Protection Requirements

Protection factors	**SD%**	**D%**	**N%**	**A%**	**SA%**	**Mean**	**Std Deviation**
Does the e-learning platform at your university have a protection facility	5.6	4.4	3.3	5.6	81.1	4.5222	1.12408
Does the e-learning platform provide for login password verification	4.4	5.6	3.3	6.7	80.0	4.5317	1.09368
Are there antivirus and or firewalls security features on the e-learning platforms	6.7	2.2	5.6	5.6	80.0	4.5103	1.14411
Total Averages	5.57	4.1	4.1	5.97	80.4	4.5214	1.12062

Source: Research Data (2021)

The study sought to establish whether the e-learning platforms in the institutions had protection facility. From the table above, the results indicated that 5.6% respondents Strongly Disagreed, 4.4% Disagreed, 3.3% remained neutral, 5.6% agreed and 81.1 Strongly Agreed with a mean of 4.5222 and standard deviation of 1.12408. Further, the responses indicated that the protection facility provided login password verification with mean of 4.5317 and standard deviation of 1.09368. Lastly, the facility had antivirus and firewalls features with mean of 4.5103 and standard deviation of 1.14411. The total average indicated a mean of 4.5214, which was a Strongly Agreed position that protection strongly affects effective management of cybersecurity on e-learning platforms in the Public Universities.

.

4.10.3 Effect of Detection on e-learning platforms in public Universities in Kenya

The study sought to establish from respondents effects of detection facility on elearning platforms, see results in the table below.

DESCRIPTIVE ANALYSIS FOR DETECTION REQUIREMENTS

Table 14: Detection Requirements

Detection factors	**SD%**	**D%**	**N%**	**A%**	**SA%**	**Mean**	**Std Deviation**
Does e-learning platforms have inbuilt Detection facility for threats for effective cyber security management	2.2	5.6	5.6	2.2	84.4	4.6111	0.9795
Does the e-learning platform have capability to check anomalies and report events	5.6	4.4	1.1	5.6	83.3	4.5667	1.1021
Does the detection facility have inbuilt cyber security corrective processes	4.4	5.6	2.2	7.8	80.0	4.5333	1.0830
Total Averages	4.07	5.2	2.97	5.2	82.6	4.5704	1.0549

Source: Research Data (2021)

Respondent had diverse opinions with regard to detection facility as shown in Table 14 where 2.2% Strongly Disagreed, 5.6% Disagree, 5.6% remained neutral, 2.2% Agreed and 84.4% Strongly Agreed. Majority agreed to this statement that elearning platforms in their institutions had detection facility for threats with a mean of 4.6111 and standard deviation of 0.9795. Furthermore, responses indicate that detection facility in e-learning platforms have capability to detect anomalies and report on events where 83.3% of respondents strongly Agreed and had a mean of 4.5667 and standard deviation 1.1021. Finally, detection facility had inbuilt cyber security corrective processes where 80% Strongly Agreed and had a mean of 4.5333 and standard deviation 1.0830. The total averages indicate the mean was 4.5704 an indication that respondents strongly agreed that detection affects e-learning in Universities. The total average standard deviation was 1.0549. The findings implied that there is a strong view from the respondents that detection is key in effective management of cyber security on elearning platforms in public universities.

4.10.4 Effect of response on e-learning platforms in public universities

The study also sought to find out the effect of response facility on e-learning platforms in the table below.

DESCRIPTIVE STATISTICS FOR RESPONSE REQUIREMENTS

Table 15: Response Requirements

Response factors	**SD%**	**D%**	**N%**	**A%**	**SA%**	**Mean**	**Std Deviation**
Does e-learning platforms have incident Response planning facility when threats are detected or occur	5.6	3.3	3.3	7.8	80.0	4.5033	1.0934
Does the response facility allow for efficient incidence turnaround time	5.6	4.4	3.3	5.6	81.1	4.5163	1.1241
Does the response facility have an inbuilt cyber security audit logs reporting system	3.3	4.4	11.1	8.9	72.2	4.4222	1.0703
Total Averages	4.83	4.03	5.9	7.4	77.8	4.4806	1.0959

Source: Research Data (2021)

Results in Table 15 indicates that the 5.6% Strongly Disagreed, 3.3% Disagreed, 3.3% remained neutral, 7.8% agreed and 80% Strongly Agreed which gave a mean of 4.5033 and standard 1.0934.This implies that the respondents strongly agreed that elearning platforms have incident response planning facility when threats are detected or occur. Further, the facility allows for efficient turnaround time where 81.1% strongly agreed and had mean of 4.5163 and standard deviation of 1.1241. Lastly, the response facility had audit logs reporting module where 72.2% strongly Agreed and had mean of 4.4222 and standard deviation of 1.0703. The total average means was 4.4806 and standard deviation of 1.0959. a strong indication that response affects effective management of cyber security on e-learning platforms in public universities Kenya.

4.10.5 E-Learning platforms requirements

DESCRIPTIVE ANALYSIS FOR E-LEARNING PLATFORMS REQUIREMENTS

Table 16: ELearning Requirements

E-learning platforms	**SD%**	**D%**	**N%**	**A%**	**SA%**	**Mean**	**Std Deviation**
Does the e-learning platform provide for effective data system integrity	2.2	12	4.4	2.2	78.9	4.433	1.1617

Source: Research Data (2021)

Table 16 indicates that e-learning platform provides for effective data system integrity with mean 4.433 and standard deviation 1.1617. This indicates that respondents strongly agreed that data system integrity is paramount in e-learning platforms.

4.10.6 Skills and User Compliance Requirements

DESCRIPTIVE ANALYSIS FOR USER COMPLIANCE AND SKILLS REQUIREMENTS

Table 17: User Compliance & User skills

User compliance and skills factors	**SD%**	**D%**	**N%**	**A%**	**SA%**	**Mean**	**Std Deviation**
Skills affects management of cyber security on e-learning platform	4.4	1.8	3.3	4.4	86.1	4.6778	0.94605
Does user compliance affect management of cyber security on e-learning platform	6.0	3.3	5.3	12	73.4	4.5111	1.03038
Total Averages	5.2	2.6	4.3	8.2	79.8	4.5945	0.98822

Source: Research Data (2021)

Table 17 indicated that skills affected management of cyber security on e-learning platforms with mean of 4.6778 and standard deviation of 0.94605. Furthermore, user compliance affects management of cyber security on e-learning platforms with mean 4.5111 and standard deviation of 1.03038. The total average mean was 4.5945 that indicated a strongly agreed position that skills and user compliance affects cyber security on e-learning platforms with total average standard deviation of 0.98822.

4.11 Inferential statistics

Regression analysis consisted of inferential statistics in this study

4.11.1 Regression Analysis

Regression analysis was performed on the influence of the independent variables in predicting the dependent variable.

Table 18: Anova

R	R Square	Adjusted R Square	Std. Error of the Estimate
.798[a]	.636	.580	.75310

Source: Research Data (2021)

Table18 .The model summary indicates that independent variables jointly accounted for 63.6% (R-Square=.636) of variation on effective management of cyber security on elearning platforms (dependent variable) 36.4 of variation in effective management of cyber security on elearning was unexplained for and this covered by factors not considered by this research.

Table 19: Analysis of Variance

	Sum of Squares	df	Mean Square	F	Sig.
Regression	76.429	12	6.369	11.230	.000[b]
Residual	43.671	77	.567		
Total	120.100	89			

The ANOVA results on Table 19 showed an F statistic value of (12,77)= 11.230 at p-value of 0.00. This implies that the model was significant at P <0.05 significance level. This indicates that the independent variables under study (Identity, Protection, Detection, Response) were statistically significant in predicting the dependent variable. (Effective management of cyber security on e-learning platforms). Additionally, unstandardized and standardized coefficients were determined from the model indicated in Table 4- 16.

Table 20: Coefficients for Predictor variable

	Unstandardized Coefficients		Standardized Coefficients		
	B	Std. Error	Beta	T	Sig.
(Constant)	0.209	0.916		0.228	0.82
Identity	0.575	0.761	0.805	0.755	0.002
Protection	0.653	0.697	0.815	0.936	0.00000
Detection	3.592	0.770	0.185	4.666	0.00001
Response	2.372	0.710	0.427	3.341	0.00124

Source: Research Data (2021)

Results in the Table 20 indicates protection had a significant effect in predicting e-learning platforms (β = 0.653; P = 0.000) implying that protection positively and significantly predicted effective management of elearning platforms. 1 unit positive change in protection would result to an increase of 0.653 in the effective management of elearning platforms (predicted variable). Results indicated detection had a significant effect in predicting effective management on e-learning platforms (β = 3.592; P = 0.000). This indicated that a unit positive change in the predictor variable detection would result in a change in the predicted variable by 3.592. Further, identity had a significant effect in predicting e-learning platforms (β = 0.575; P = 0.002). This indicated that a change in the predictor variable identity by one unit would result in a change in the predicted variable by a margin of 0.575. Finally, response had a significant effect in predicting the dependent variable (β = 2.372; P = 0.00124). This showed that an increase in the predictor variable response would cause a change of 2.2372 in the predicted variable.

Table 20 Beta coefficients results indicated that protection had the largest effect on β = 0.815, followed by identity β =0.805, response β =0.427 and finally detection β =0.185

The regression model obtained before including the moderating variables (MV1, MV2) was of the form.

$Y=\alpha+ \beta_1 X_1+ \beta_2 X_2+ \beta_3 X_3+ \beta_4 X_4$

Where Y= Dependent variable β = are unknown values X_1 = Identity (I) X_2 = Protection (P) X_3 = Detection (D) X_4= Response (R)

Y= 0.209 + 0.575I+0.653P+3.592D+2.372R

Regression model using User compliance as moderating variable (MV1)

Table 21: Regression Model Fitness User Compliance (MV1)

R	R Square	Adjusted R Square	Std. Error of the Estimate
.819[a]	.671	.615	.72072

Table 21 indicated the adjusted R^2 change of 0.671 in the regression model, which explained 67.1% when included in predicting the dependent variable. The results means that the user compliance moderator variable applied in the model to link the relationship of the variables was satisfactory and had a positive influence in predicting the outcome of the dependent variable.

ANOVA Moderated model MV1 user Compliance

Table 22: Anova Moderator MV1

	Sum of Squares	df	Mean Square	F	Sig.
Regression	80.623	13	6.202	11.939	.000[b]
Residual	39.477	76	.519		
Total	120.100	89			

Table 22 indicates the results on the (ANOVA). The F statistic was 11.939 and p = 0.000 which was less than the probability 0.05 significant level, thus the results indicate that the model was statistically significant in predicting the dependent variable.

TABLE 4- 19: REGRESSION MODEL FITNESS SKILLS (MV2)

Table 23 : Regression Model Fitness Skill

R	R Square	Adjusted R Square	Std. Error of the Estimate
.814[a]	.663	.606	.72944

Table 23 indicated the adjusted R^2 change of 0.663 in the regression model, which explained 66.3%

when included in predicting the dependent variable. The results means that the skill moderator variable applied in the model to link the relationship of the variables was satisfactory and had a positive influence in predicting the outcome of the dependent variable.

ANOVA Moderated model MV2 skill

Table 24: Anova Moderator skills MV2

	Sum of Squares	df	Mean Square	F	Sig.
Regression	79.662	13	6.128	11.517	.000[b]
Residual	40.438	76	.532		
Total	120.100	89			

Table 24 indicates the results on the (ANOVA). The F statistic was 11.517 and p = 0.000 which was less than the probability 0.05 significant level, thus the results indicate that the model was statistically significant in predicting the dependent variable.

Table 25: Regression Model after Moderation

	Unstandardized Coefficients		Standardized Coefficients		
	B	Std. Error	Beta	t	Sig.
(Constant)	0.2282	0.8826		.259	.797
Identity	0.9871	0.7769	0.7430	1.2705	0.0070
Protection	0.0709	0.8184	0.9390	0.0867	0.03100
Detection	3.3808	0.8677	0.2280	3.8962	0.39100
Response	2.1022	0.8106	0.5010	2.5935	0.01121
MV 1, 2	3.5081	.61815	0.1800	5.6751	.0000002

Source: Research Data (2021)

Optimal model after moderation

$$\mathbf{Y = 0.2282+0.9871X_1+0.0709X_2+3.3808X_3+2.1022X_4+3.5081MV\ (1+2)}$$

Where Y= Dependent variable

X_1 = Identity (I)

X_2 = Protection (P)

X_3 = Detection (D)

X_4= Response (R)

MV (1+2) = User Compliance + User skills

4.11.2 Discussion of the findings

The findings from the sections 4.10.1 to 4.10.6 above identified Effect of identity on elearning platforms in public universities, Effect of Protection on e-learning platforms in public Universities, Effect of Detection on e-learning platforms in public Universities, Effect of Response on e-learning platforms in Public universities, E-Learning Platforms Requirements and Skills & User Compliance Requirements**.**

The regression analysis results captured in table 25 after moderation indicated that detection had a regression coefficient of β =3.3808 and p=0.39100, implying that user compliance and user skills significantly enhanced detection in predicting effective management of cybersecurity on elearning platforms. 1 unit positive change in detection would lead to an increase of 3.3808 units in effective management of cybersecurity on elearning platforms.

The findings are underpinned by studies conducted by (Saeed et al., 2021) that suggested that threat detection is critical and must be done as a constant monitoring and evaluation procedure to check on threats that may have been detected previously and can be handled better next time through set up of measures such as firewalls and protection software.

Further, after moderation response had a regression coefficient of β =2.1022 and p=0.01121, implying that moderation enhanced response in predicting the dependent variable. 1unit positive change in response would lead to an increase of 2.1022 units in effective management of cybersecurity on elearning platforms.

This finding compares with Ulven and Wangen (2021) who opined that on response mechanism, institutions should have to include implementing mitigation measures such as conducting backups.

Identity had regression coefficient of β =0.9871 and p = 0.0070, implying that identity is statistically significant in predicting the dependent variable and a 1 unit positive change in identity would lead to an increase of 0.9871 units in effective management of cybersecurity on elearning platforms. This findings compares with the study conducted by (Bandaras, loras & Maher, 2014) who posits that it is imperative for institutions to have identifiers that prevent unauthorized access of data by others through falsification, intrusion and even tutors getting personal data for students.

Protection after moderation had regression coefficients of β =0.0709 and p=0.03100, implying that identity was significant in predicting the dependent variable and a 1 unit positive change in protection would to an increase of 0.0709 units in effective management of cybersecurity on elearning platforms. This findings support the studies carried out by (Ford, 2016) which suggests that protection is imperative in building digital trust by users. Additionally, protection helps protect cyber theft and avoid remote exploitation that helps in data protection.

Lastly, the moderating variable had a significant effect on the dependent variable with a regression coefficient of β =3.5081 and p=0.0000002.

4.12 Multi-collinearity tests

Multi-collinearity was tested on the variables in the mode, items are said to be collinear when they are correlated Kothari (2010). This becomes a problem when variables are similar and seem to measure the same feature. Testing for Multi-collinearity was done by observing the Variance Inflation Factors (VIF) or the tolerance. According to (Hair et al, 1995) homogeneity presumes the dependent variable shows similar amounts of variance across the range of values min the group of tests. Table 4- 22 depicts items having VIF of less than two indicating no presence of Collinearity in items within the model.

Table 26: Collinearity Statistics

Coefficients		
	Collinearity Statistics	
	Tolerance	VIF
Identifier Module	.700	1.428
Threat Detection	.826	1.211
Authorization levels	.733	1.364
Protection Facility	.699	1.431
Password Verification	.860	1.163
Antivirus Or Firewall	.557	1.796
Inbuilt Detection	.722	1.386
Anomalies and Reporting	.675	1.482
Corrective Process	.724	1.380
Incidence Response	.554	1.806
Efficient Turnaround time	.636	1.571
Audit Log Reporting	.746	1.341

Source: Research Data (2021)

4.13 Skewness and Kurtosis

The study tested how the curve was distributed from the mid-point. According to (Kim, 2013) skewness is a measure of asymmetry whereas kurtosis measures the peakness of a distribution. Further (Byrne, 2010) posit that the range of values of data is considered normal if Skewness is between -2 to +2 and Kurtosis is between -7 to +7. Table 4- 23 indicates skewness and kurtosis of items and values fall within the range. This was used in determining the normality curve of the standard regression residuals indicated in figure 8

Descriptive statistics

Table 27: Descriptive Statistics

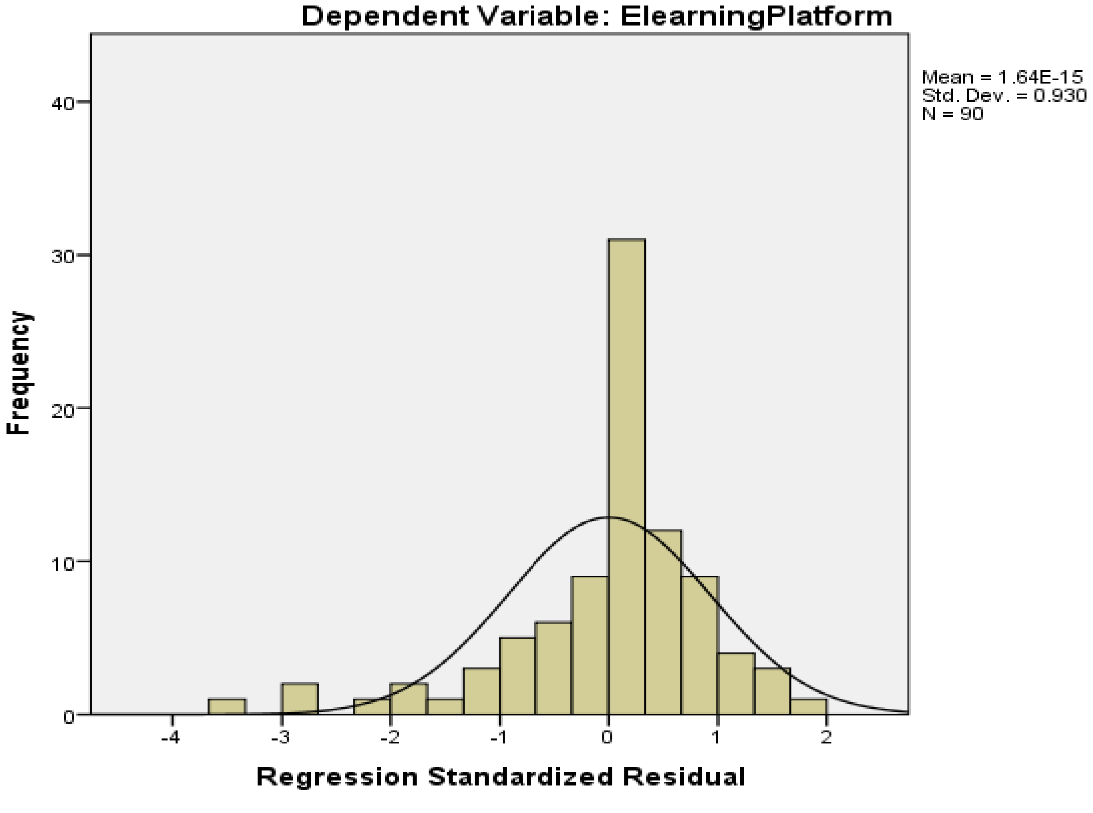
	N	Minimum	Maximum	Mean	Std. Deviation	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
Identifier Module	90	1.00	5.00	4.4667	1.12380	-2.125	.254	3.429	.503
Threat Detection	90	1.00	5.00	4.5111	1.01941	-2.406	.254	5.159	.503
Authorization levels	90	1.00	5.00	4.5222	1.06241	-2.216	.254	3.735	.503
Protection Facility	90	1.00	5.00	4.5222	1.12408	-2.314	.254	4.061	.503
Password Verification	90	1.00	5.00	4.5222	1.09368	-2.272	.254	3.939	.503
Antivirus or Firewall	90	1.00	5.00	4.5000	1.14411	-2.279	.254	3.972	.503
Inbuilt Detection	90	1.00	5.00	4.6111	0.97950	-2.447	.254	4.838	.503
Anomalies and Reporting	90	1.00	5.00	4.5667	1.10209	-2.517	.254	4.978	.503
Corrective Process	90	1.00	5.00	4.5333	1.08307	-2.340	.254	4.272	.503
Incidence Response	90	1.00	5.00	4.5333	1.09339	-2.408	.254	4.662	.503
Efficient turnaround time	90	1.00	5.00	4.5222	1.12408	-2.314	.254	4.061	.503
Audit Log Reporting	90	1.00	5.00	4.4222	1.07031	-1.817	.254	2.370	.503
E-learning Platform	90	1.00	5.00	4.4333	1.16165	-1.748	.254	1.436	.503
Valid N (listwise)	90								

Source: Research Data (2021)

Regression Standardized Residuals

According to (Cohen et al., 2002) normality is tested to identify model inappropriately influential cases. This enables one to determine the extent to which the curve is normally distributed from the mid-point. Figure 8 shows that the values in the unstandardized residuals were distributed along the expected normal curve. Utilizing the ranges of the skewness and Kurtosis, the standard regression residual curve was seen to be normally distributed. This was an indication that the curve distribution was normal, this was an indication that the data were distributed closer to the mean statistic position. Table 27 indicates the minimum statistic from one and the maximum statistic as five. The distribution of the mean statistic was above 4.4 indicating the normality of the curve distributed about the mean position. Figure 8 indicates the normality of the curve distributed using the values of statistic skewness and kurtosis represented in Table 27.

Figure 8 : Histogram of Regression Standardized residuals



Source: Research Data (2021)

4.14 Hypotheses testing

The model achieved good fit and all the tolerance levels were met. The moderating factors (user Compliance and User skills) was added to see their effect on the model. From the analysis results, it had significant effect on moderating independent variables to predicting dependent variable.

Based on the findings **HO1** null hypothesis is rejected and the alternative hypothesis is accepted indicating that there is significant effect of identity on effective management of cybersecurity on e-learning platforms in Public Universities in Kenya

Based on the findings **HO2** null hypothesis is rejected and the alternative hypothesis is accepted indicating that there is significant effect of protection on effective management of cybersecurity on e-learning platforms in Public Universities in Kenya

Based on the findings **HO3** null hypothesis is rejected and the alternative hypothesis is accepted indicating that there is significant effect of detection on effective management of cybersecurity on e-learning platforms in Public Universities in Kenya.

Based on the findings **HO4** null hypothesis is rejected and the alternative hypothesis is accepted indicating that there is significant effect of response on effective management of cybersecurity on e-learning platforms in Public Universities in Kenya.

The moderating variable **H05** Null hypothesis is rejected that there is no effect of user skills and user compliance on effective management of cybersecurity on e-learning platforms in Public Universities in Kenya using e- learning platforms. This is based on the findings from the study which established that user compliance affects e-learning platforms the higher the user compliance and knowledge of usage of the platforms the greater the efficiency in the platforms and vice versa, this is underscored by a study conducted by Oyediran (2020). The study revealed that user compliance is a key driver towards the success of e-platforms. Moreover (Andreas, 2020) postulates that advanced education and ICT skills are important given the radical shift towards online e–learning platforms. This concurs with the study findings that skills are important and affect e-learning platforms, and hence users must be equipped and be conversant with the new paradigm shift towards electronic platforms as a way of management as a result the alternative hypothesis is accepted that there is an effect of user skills and user compliance on effective management of cybersecurity on e-learning platforms in Public chartered Universities in Kenya.

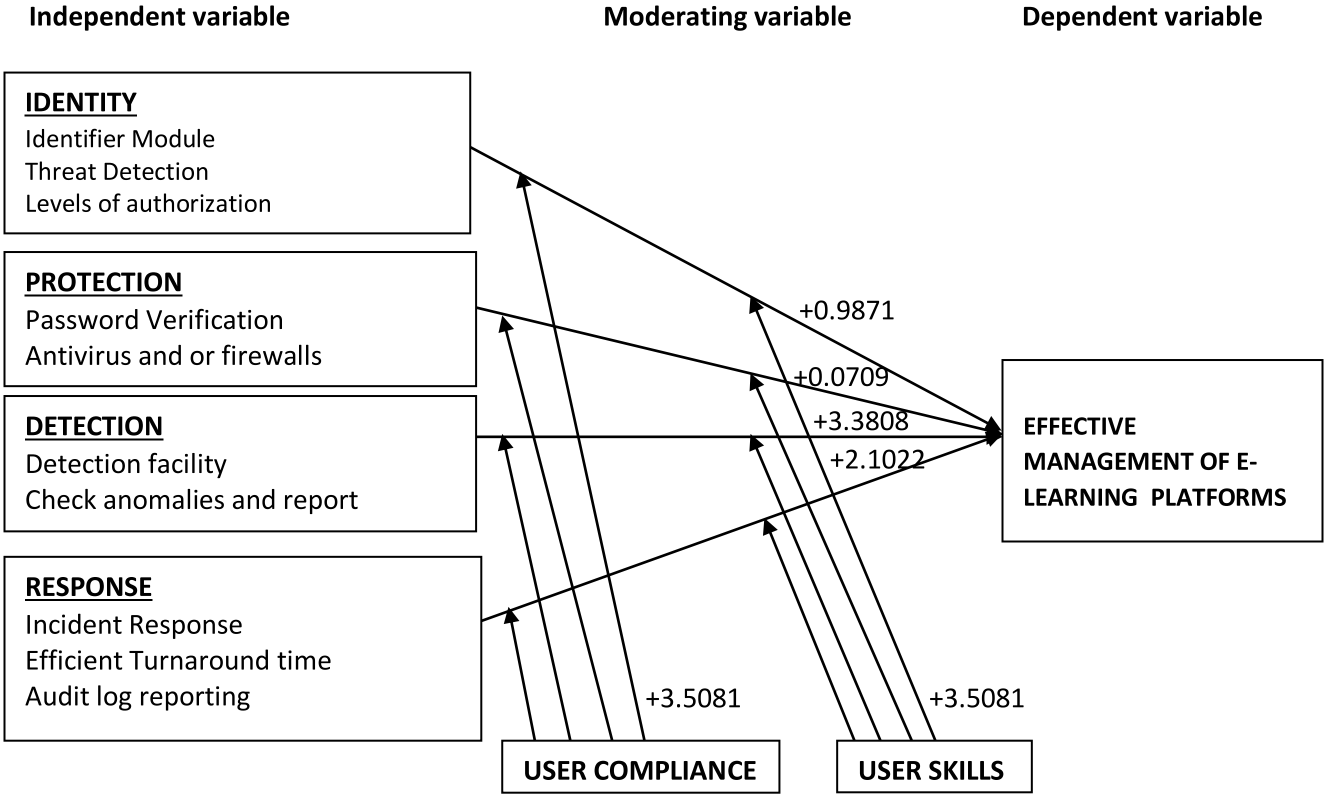
Table 28: Summary Hypothesis

Hypothesis	Test Criteria	Findings	Conclusion
HO$_1$: There is no significant effect of identity on effective management of cybersecurity on e-learning platforms in Public Universities in Kenya	Reject hypothesis if P-Value is ≤ significant value 0.05	P-value= 0.002 ≤ (0.05)	Reject the hypothesis and accept alternative
HO$_2$: There is no significant effect of protection on effective management of cybersecurity on e-learning platforms in Public Universities in Kenya	Reject hypothesis if P-Value is ≤ significant value 0.05	P-value= 0.00000 ≤ (0.05)	Reject the hypothesis and accept alternative
HO$_3$: There is no significant effect of detection on effective management of cybersecurity on e-learning platforms in Public Universities in Kenya	Reject hypothesis if P-Value is ≤ significant value 0.05	P-value= 0.00001 ≤ (0.05)	Reject the hypothesis and accept alternative
HO$_4$: There is no significant effect of response on effective management of cybersecurity on e-learning platforms in Public Universities in Kenya	Reject hypothesis if P-Value is ≤ significant value 0.05	P-value= 0.00124 ≤ (0.05)	Reject the hypothesis and accept alternative
HO$_5$: There is no significant relationship of the joint effect of the moderating variable user compliance and user skills on effective management of cybersecurity on e-learning platforms in Public Universities in Kenya	Reject hypothesis if P-Value is ≤ significant value 0.05	P-value= 0.000002 ≤ (0.05)	Reject the hypothesis and accept alternative

Arising from the foregoing discussions from regression and descriptive analysis, all factors considered in this study positively predicted effective management of cybersecurity on e-learning platforms. This means that there would be some positive change in effective management of cybersecurity on e-learning platforms for every unit increase in these factors.

Figure 9. Below is an illustration of the constructed model using the regression analysis results findings. Subsequently, the model together with descriptive analysis results findings were used to come-up with appropriate framework that can effectively manage cybersecurity on e-learning platforms. The identified framework is illustrated in figure 10. This framework can be used by cybersecurity experts to promote cybersecurity culture in public universities.

Figure 9: New Conceptual framework



The regression model after inclusion of the moderating variables was of the form:

$Y=\alpha+\beta_1 X_1+\beta_2 X_2+\beta_3 X_3+\beta_4 X_4+\beta_5$ MV (1+2)

Y = $0.2282+0.9871X_1+0.0709X_2+3.3808X_3+2.1022X_4+3.5081$MV (1+2)

Where Y= Dependent variable

X_1 = Identity (I)

X_2 = Protection (P)

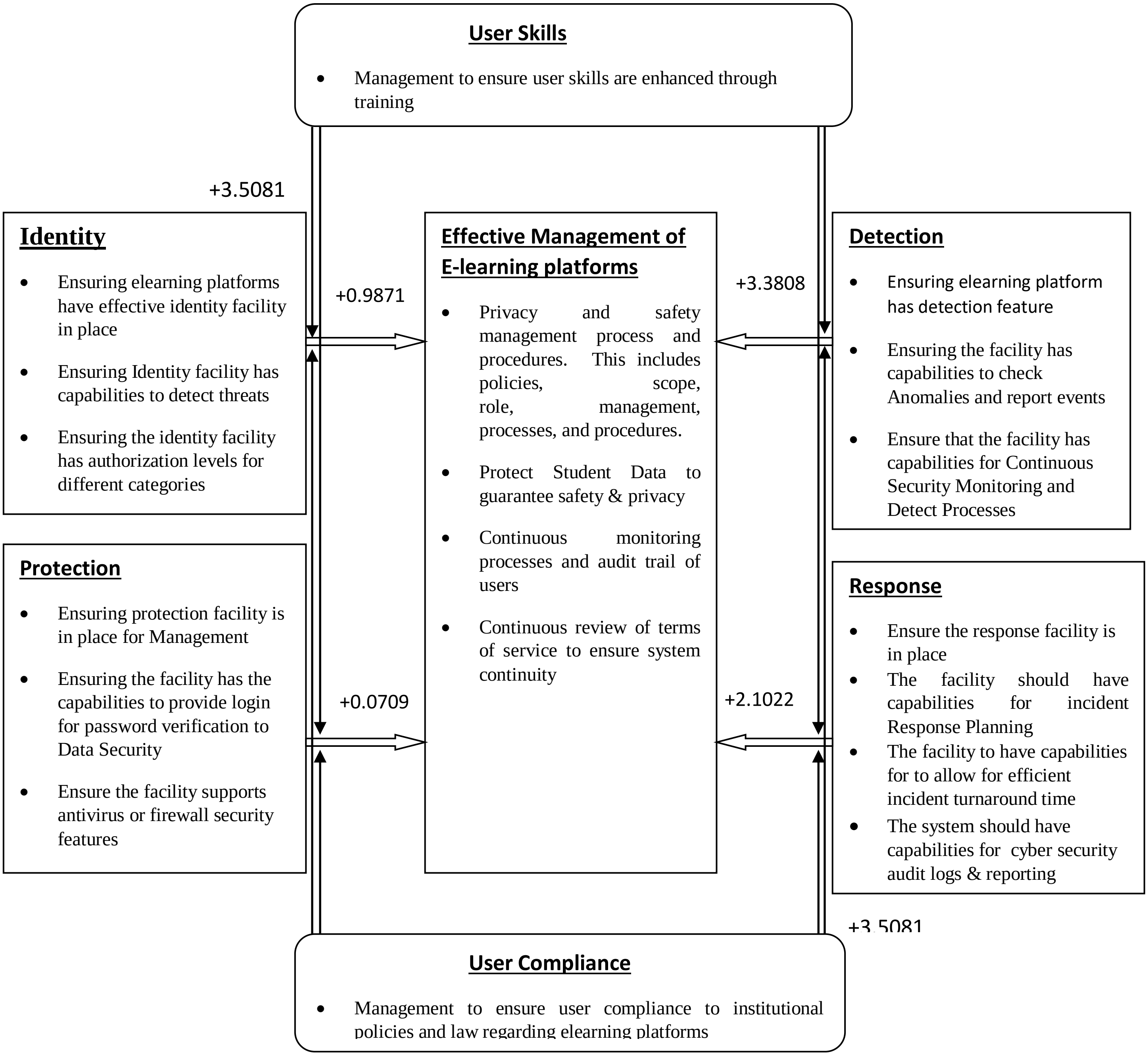
X_3 = Detection (D)

X_4= Response (R)

MV (1+2) = user compliance+ User skills

$\beta_1, \beta_2, \beta_3, \beta_4$ are independent variable coefficients

Figure 10: Framework For Effective Management Of Cyber Security On E-Learning Platforms In Public Universities In Kenya



User Skills

- Management to ensure user skills are enhanced through training

Identity

- Ensuring elearning platforms have effective identity facility in place
- Ensuring Identity facility has capabilities to detect threats
- Ensuring the identity facility has authorization levels for different categories

Protection

- Ensuring protection facility is in place for Management
- Ensuring the facility has the capabilities to provide login for password verification to Data Security
- Ensure the facility supports antivirus or firewall security features

Effective Management of E-learning platforms

- Privacy and safety management process and procedures. This includes policies, scope, role, management, processes, and procedures.
- Protect Student Data to guarantee safety & privacy
- Continuous monitoring processes and audit trail of users
- Continuous review of terms of service to ensure system continuity

Detection

- Ensuring elearning platform has detection feature
- Ensuring the facility has capabilities to check Anomalies and report events
- Ensure that the facility has capabilities for Continuous Security Monitoring and Detect Processes

Response

- Ensure the response facility is in place
- The facility should have capabilities for incident Response Planning
- The facility to have capabilities for to allow for efficient incident turnaround time
- The system should have capabilities for cyber security audit logs & reporting

User Compliance

- Management to ensure user compliance to institutional policies and law regarding elearning platforms

CHAPTER FIVE

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter presents a summary of the study findings, conclusions. The chapter also highlights recommendation and suggestions for further research.

5.2 Summary of major findings

This research aimed at establishing the framework for effective management of cyber security on e-learning platforms in public universities in Kenya. The specific objectives were; To examine the effect of identity on effective management of cybersecurity on e-learning platforms, examine the effect of protection on effective management of cyber security on e-learning platforms, examine the effect of detection on effective management of cybersecurity on e-learning platforms, examine the effect of response on effective management of cyber security on e-learning platforms. The study also sought to establish the joint effects of user skills and user compliance on effective management of cybersecurity on e- learning platforms.

Objective1: To establish the effect of identity on effective management of cybersecurity on e-learning platforms in public universities in Kenya.

The research question was answered through administration of questionnaires. The data was analyzed through descriptive analysis in section 4.10.1 and through regression analysis in section 4.11.1 see table 20 and 25. The findings in descriptive analysis indicated strong response that identity influenced effective management of cyber security on elearning platforms. Regression analysis also indicated that identity was statistically significant in predicting effective management of elearning platforms as well as the revised research model in chapter 4 of this document.

The study established that identity had an effect on e-learning platforms. This findings compares with the study conducted by (Bandaras, loras & Maher, 2014) which posits that it is imperative for institutions to have identifiers that prevent unauthorized access of data by others through falsification, intrusion and even tutors getting personal data for students.

Objective2: To establish the effect of protection on effective management cybersecurity on e-learning platforms in public universities in Kenya.

The research question was addressed using the research findings of the descriptive and regression analysis. The descriptive analysis from the data gathered from research instrument showed strong response that protection affected effective management of cyber security on elearning platforms section 4.10.2 and the regression analysis in section 4.11.1 indicated that protection was statistically significant in predicting effective management of cybersecurity on elearning platforms. The framework was as presented in figure chapter 4 of this document.

This findings compares with the studies carried out by (Ford, 2016) that suggested that protection is imperative in building digital trust by users. Additionally, protection helps protect cyber theft and avoid remote exploitation that helps in data protection.

Objective3: To establish the effect of detection on effective management of cybersecurity on e-learning platforms in public universities in Kenya.

The objective was addressed using research findings of the regression analysis as well data from descriptive analysis. The descriptive analysis of the data collected from research instrument revealed that detection strongly affected effective management of cybersecurity on elearning platforms section 4.10.3. Regression analysis results in section 4.11.1 indicated that detection was statistically significant and positively influenced management of cybersecurity on elearning platforms as presented in figure in chapter 4 of this document.

The findings are underpinned by studies conducted by (Saeed et al., 2021) that suggested that treat detection is critical and must be done as a constant monitoring and evaluation procedure to check on threats that may have been detected previously and can be handled better next time through set up of measures such as firewalls and protection software.

Objective4: of the study sought to establish the effect of response effective management of cybersecurity on e-learning platforms in public universities in Kenya.

The objective was addressed using research findings of the descriptive analysis where respondent strongly agreed that it affected effective management of cybersecurity on elearning platforms section 4.10.4. Regressional analysis results also indicated that response was statistically significant in predicting effective management of cybersecurity on elearning platforms section 4.11.1. This informed the developed framework in chapter 4 of this document.

The study established that response is critical in e-learning platform to protect data loss. The study is supported by Ulven and Wangen (2021) who opined that on response mechanism, institutions should have to include implementing mitigation measures such as conducting backups.

Objective5: To establish whether moderating effect of user skills and user compliance contributed to effective management of cybersecurity on e- learning platforms in public universities in Kenya.

The findings from both descriptive and regression analysis indicated that the two moderating variables positively moderated independent variables in predicting dependent variable which is evident in figure 9. In chapter 4 of this document.

The study established that user compliance affects e-learning platforms, the higher the user compliance and knowledge of usage of the platforms the greater the efficiency in the platforms and vice versa, this is underscored by a study conducted by Oyediran (2020). The study revealed that user compliance is a key driver towards the success of e-platforms. Moreover (Andreas, 2020) postulates that IT knowledge is important due to paradigm shift to e–learning platforms. This concurs with the study findings that skills are important and affect e-learning platforms, and hence users must be equipped and be conversant with the new paradigm shift towards electronic platforms as a way of management.

What is new?

The study posits that cybersecurity management on e-learning is dependent on people who are the weakest link as they are source of cybersecurity threats. It affirms that the higher the user skills and compliance to policies, the lower the cyber risks. There is need for training and sensitization of users and stakeholders in the cybersecurity management process.

Who else could be interested in this study apart from academicians?

Institutions can adopt this research recommendation to combat cybercrime. Regulatory bodies also can use this research to identify key areas to focus on to improve cybersecurity management.

5.2 Conclusion of the study

The research findings stemming from descriptive and regression analysis revealed that the developed framework if deployed would enhance management of cybersecurity on elearning platforms in institutions of higher learning.

User compliance to policies and laws set and user skills play a crucial role in mitigating cybercrimes on elearning platforms.

Identity, protection, detection and response are significant for effective management of cybersecurity on elearning platforms.

5.3 Recommendation

The study therefore recommends the multipronged approach in securing the users of elearning platforms by developing frameworks that are relevant and adaptive to the changing cyberspace.

The laid down procedures, processes, and policies need to be adhered to safeguard the elearning platforms, it's assets to ensure Confidentiality, Integrity and Availability is guaranteed.

There is need to sensitize and train the users of elearning systems to enhance their skills and compliance when using elearning platforms to reduce cybercrime threats.

The need for the university to invest on cybersecurity to ensure students data, lecturers and management data is secured.

5.4 Suggestion for further Research

It was established that the model accounted for 63.6% of variation in effective management of cybersecurity on e-learning platforms. Further study should focus on a wide scope to explain the remaining 36.4% variation in effective management of cybersecurity on elearning. Similar studies to be conducted in private universities across the country.

REFERENCES

Andreas, S., (2020). The Impact of COVID-19 on Education - Insights from Education at a Glance 2020. OECD, p. 31.

Airehrour, D., & Nair,N,V. & Madanian, S. (2018).Social Engineering Attacks and Countermeasures in the New Zealand Banking System: *Advancing a User-Reflective Mitigation Model.*

Abdulrahim, N. (2019). Managing Cybersecurity as a Business Risk in Information Technology-based Smes (Doctoral dissertation, University of Nairobi).

Abdullah, M. S., Toycan, M., & Anwar, K. (2017). The cost readiness of implementing elearning. CustosE Agronegocio on Line, 13(2), 156-175.

Bada, J. K., Asianzu, E., Lugemwa, B., Namataba, J., & Milburga, A. (2020). An Empirical Study on ELearning Uptake by Teaching Staff at Makerere University Business School.

Bandara, I., Ioras, F., & Maher, K. (2014). Cyber security concerns in e-learning education

Blumberg, B., Cooper, D., & Schindler, P. (2014). EBOOK: Business Research Methods. McGraw Hill.

Bazimaziki, G. (2020). Challenges in using ICT Gadgets to cope with effects of COVID-19 on Education: A short survey of online teaching Literature in English. Journal of Humanities and Education Development (JHED), 2(4), 299-307.

Byrne, B. M. (2010). Structural Equation Modeling with Amos: Basic Concepts, Applications, and Programming (2nd ed.). New York: Taylor and Francis Group.

Baillette, P., & Barlette, Y. (2018). BYOD-related innovations and organizational change for entrepreneurs and their employees in SMEs. *Journal of Organizational Change Management*.

Carliner, S., & Shank, P. (Eds.). (2016). The e-learning handbook: past promises, present challenges. John Wiley & Sons.

Cooper, D. R. & Schindler, P.S. (2011). *Business research methods (11th ed.). New York: McGraw-Hill.*

Chimi, C. J., & Russel, D. L. (2009). The Likert Scale: a proposal for improvement using quasi-continuous variable. In the proceedings of the information systems education conference, Washington DC 1542-7382.

Chairoel, L., & Widyarto, S., & Pujani, V. (2015). ICT adoption in affecting organizational performance among Indonesian SMEs. *The International Technology Management Review Vol. 5* (2015)(No. 2):82-93

Chitrey A., Singh D., Bag M. and Singh V. (2012). A Comprehensive Study of Social Engineering Based Attacks in India to Develop a Conceptual Model. International Journal of Information & Network Security (IJINS)

Cohen, J., Cohen, P., West, S., & Aiken, L. S. (2002). Applied Multiple Regression/Correlation Analysis for the Behavioral Sciences.

Cardenas, R. G., & Sanchez, E. M. (2005). Security challenges of distributed e-learning systems. In International Symposium and School on Advanced Distributed Systems (pp. 538-544). Springer, Berlin, Heidelberg.

Coffey, J. W., Haveard, M., & Golding, G. (2018). A case study in the implementation of a human-centric higher education cybersecurity program. Journal of Cybersecurity Education, Research and Practice.

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. *NIST Special Publication*, *800*(61), 1-147.

De Haes, S., Van Grembergen, W., Joshi, A., & Huygh, T. (2020). Enterprise Governance of Information Technology: Achieving Alignment and Value in Digital Organizations.

Drost, E. A. (2011). Validity and Reliability in Social Science Research. Education Research and Perspectives, 38(1), 105-123.

Fischhoff, B. (1995). Risk perception and communication unplugged: twenty years of process 1. Risk analysis, 15(2), 137-145.

Fovino I. N., Barry G., Chaudron S., Coisel I., Dewar M., Junklewitz H., Kambourakis G., Kounelis I., Mortara B., Nordvik J.p., Sanchez I. (Eds.), Baldini G., Barrero J., Coisel I., Draper G., Duch-Brown N., Eulaerts O., Geneiatakis D., Joanny G., Kerckhof S., Lewis A., Martin T., Nativi S., Neisse R., Papameletiou D., Ramos J., Reina V., Ruzzante G., Sportiello L., Steri G., & Tirendi S., (2020). Cybersecurity, our digital anchor. EUR 30276 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-19957-1, doi: 10.2760/352218, JRC121051

Ghernaouti-Helie, S. (2019). *Cyber power:* Crime, conflict and security in cyberspace. .

Hwang, D. J., Yang, H. K., & Kim, H. (2010). E-Learning in the Republic of Korea. UNESCO Institute for Information Technologies in Education. 8 Kedrova St., Bldg. 3,Moscow, 117292, Russian Federation

Hussain, M., Zaidan, A. A., Zidan, B. B., Iqbal, S., Ahmed, M. M., Albahri, O. S., & Albahri, A. S. (2018). Conceptual framework for the security of mobile health applications on android platform. *Telematics and Informatics*, *35*(5), 1335-1354.

Hair, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (1998). *Multivariate Data Analysis with Readings* (*5th ed.).* Englewood Cliffs, NJ: Prentice Hall.

Harris, J., Ives, B., & Junglas, I. (2012). IT Consumerization: When gadgets turn into enterprise IT tools. MIS Quarterly Executive, 11(3).

Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Goeke, L., Hildebrandt, T., Tsakirakis, G., Oikonomou, F., Leftheriotis, G., & Koshutanski, H. (2020). Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees. MDI *Journal of Appl. Sci.* 2020, *10, 5702*

Imgraben, J., Engelbrecht, A., & Choo, K. K. R. (2014). Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. *Behaviour & Information Technology*, *33*(12), 1347-1360.

Kundi, G. M., Nawaz, A., Akhtar, R., & MPhil Student, I. E. R. (2014). Digital revolution, cyber-crimes and cyber legislation: A challenge to governments in developing countries. *Journal of Information Engineering and Applications, 4*(4), 61-71.

Kashorda, M., & Waema, T. (2014). E-Readiness survey of Kenyan Universities (2013) report. Nairobi: Kenya Education Network.

Kothari, C. R. (2010). Research Methodology: New Delhi, KK Grupta of New Age International.

Kothari, C.R. (2004) Research Methodology Methods and Techniques. 2nd Edition, New Age International Publishers, New Delhi.

Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technology factors. MIS Quarterly executive, 9(3), 2012-52.

Kamaludeen, M., Ismaeel, S., Asiri, S., Allen, T., & Scarfo, C (2020). *A Framework for Cyber Protection (FCP) in K-12 Education Sector.*

Kombo, D. K., & Tromp, D. L. (2009). Proposal and thesis writing: An introduction. Nairobi: Don Bosco Printing press.

Moturi,C,A., & Mwasambo, L,M, . (2016), Experience in Social Engineering by eCommerce Platforms in Kenya

Mugenda, A., & Mugenda, O., (2003); Research Methods, Quantitative and Qualitative Approaches, ACTS Press, Nairobi.

Mugenda, A. G. (2008). Social science research: Theory and principles. Nairobi: Applied Research and Training Services.

Hair, J.R., R.E. Anderson, R.L. Tatham, and W.C. Black.(1995). Multivariate Data Analysis with Readings. Prentice Hall, Englewood, NJ.

Moore, J. L., Dickson-Deane, C., & Galyen, K. (2011). e-learning, online learning, and distance learning environments: Are they the same?. The Internet and Higher Education, 14(2), 129-135.

Mungai, N. W., Njuguna, V. W., Mshenga, P. M., & Mbudzya, J. J. Ruforum (2018). Working Document Series (ISSN 1607-9345), 2018, No. 17 (2): 46-53. Available from http://repository. ruforum. org.

Moşteanu, N. R. (2020). Challenges for Organizational Structure and design as a result of digitalization and cybersecurity. *The Business & Management Review*, *11*(1), 278-286.

NESC (2007). Kenya Vision 2030: A globally competitive and prosperous Kenya. National Economic and Social Council of Kenya.

Namdeo, S. K., Rout, S. D. (2016). Calculating and Interpreting Cronbach's Alpha Using Rosenberg Assessment Scale on Pediatrician's attitude and Perception on Self Esteem. *International Journal of Community Medicine and public health*, *3*(6), 1371-1374. doi: 10.18203/2394-6040

Nagy, J., Oláh, J., Erdei, E., Mate, D., & Popp, J. (2018). The role and impact of Industry 4.0 and the internet of things on the business strategy of the value chain—the case of Hungary. *Sustainability*, *10*(10), 3491.

Omolohunnu, R. (2019). Cybersecurity*:* A Nonexperimental Correlational Study of Organizational Employees' Security Perceptions and Vulnerabilities in Information Technology Infrastructure (Doctoral dissertation, Capella University).

Proceedings of ICERI2014 Conference paper. P.P 728-734.

Pierlugin Paganini (2017). Introduction to the NIST Cybersecurity Framework for a Landscape of Cyber Menaces.

Patel, S., & Zaveri, J. (2010). A risk-assessment model for cyber-attacks on information systems. J. Comput., 5(3), 352-359.

PwC, Anatomy of Social Engineering Attack, in Exploiting Human Behaviours; 2016. Team VR. Data Breach Investigations Report; 2015.

Pathak, P. B., & Nanded, Y. M. (2016). A dangerous trend of cybercrime: ransomware growing challenge. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 5(2), 371-373.

Park, S. Y. (2009). An analysis of the technology acceptance model in understanding university students' behavioral intention to use e -Journal of Educational Technology & Society, 12(3), 150-162.

Rabai L. B. A. and Rjaibi N. (2012). Quantifying Security Threats for E-learning Systems. Education and e-Learning Innovations (ICEELI), 2012 International Conference, Tunis, Tunisia, July, 2012.

Ratheeswari, K. (2018). Information Communication Technology in Education. *Journal of Applied and Advanced Research* 3(S1):45

Saeed, Rana & Alhumaid, Khadija & Akour, Iman & Salloum, Said. (2021). Factors That Affect E-Learning Platforms after the Spread of COVID-19: Post Acceptance Study. Data. 6. 49. 10.3390/data6050049.

Swiatkowska, J. (2020). Tackling cybercrime to unleash developing countries' digital potential. Pathways for Prosperity Commission on Technology and Inclusive Development, 2020-01.

Sen, J. (2013). Security and Privacy Issues in Cloud Computing Computing. Cornell University. Innovation Labs, Tata Consultancy Services: INDIA. P.P 1-42.

Trelease, R. B. (2016). From chalkboard, slides, and paper to e-learning: How computing technologies have transformed anatomical sciences education. Anatomical sciences education, 9(6), 583-602.

Uebelacker S, Quiel S. (2014). The social engineering personality framework, in 4th Workshop on Socio-Technical Aspects in Security and Trust (STAST). IEEE: Vienna, Austria. 2014;

Ulven, J.B.; Wangen, G. A. (2021). Systematic Review of Cybersecurity Risks in Higher Education. Future Internet 2021, 13, 39. https://doi.org/10.3390/fi13020039

West, S.G., Finch, J.F. and Curran, P.J. (1995) Structural Equation Models with Non Normal Variables: Problems and remedies. In: Hoyle, R.H., Ed., Structural Equation Modeling: Concepts, Issues, and Applications, Sage, Thousand Oaks, 56-75.

Leal,R. (2016). How to integrate COSO, COBIT, and ISO 27001 Frameworks

Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and society*. Sage.

Zikmund, W. G., Babin, B. J., Carr, J. C., & Griffin, M. (2012). *Business Research Methods* (9th ed.). New York: The Free Press.

Aldawood, H., & Skinner, G. (2018, December). Educating and raising awareness on cyber security social engineering: A literature review. In 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)(pp. 62-68). IEEE.

Coolican, H. (2014). Research Methods and Statistics in Psychology. London: Hugh Coolican.

INTERNET SOURCES

The star (2020). Intruders flood online classes with porn threats [online] Available at https://www.the-star.co.ke/news/2020-07-20-intruders-flood-online-classes-with-porn- threats. Accessed on June,2021

Phys.org. (2019). 30 years later, Berners-Lee sees mission to fix internet’s ills [online] Available at: https://www.phys.org/news/2019-03-years-berners-lee-missioninternet-ills.html. Accessed on March, 2019

Moodle Learning Management system (LMS) Curtin University (2002), with a focus on offering a basic collaborative, construction of content platform for technical users [online] available at: https://docs.moodle.org/. Accessed on June,2021

KenyaCyberSecurityReport2017 [online] available at
: https://www.serianu.com/downloads/KenyaCyberSecurityReport2017.Accessed on May, 2021

Technical report, vol. 21, Symantec, April 2016.[online] available at: https://docs.broadcom.com/doc/istr-21-2016-en .Accessed on April, 2021

“Internet organized crime threat assessment”, Technical report, Europol, 2016 [online] Available at: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta- 2016). Accessed on June, 2021

Internet-organised-crime-threat-assessment-iocta-2018) IOCTA 2018 [online] Available at: https://www.europol.europa.eu/activitiesservices/main-reports/internet-organised-crime-threat-assessment-iocta-2018. Accessed on June, 2021.

Hoog, A. (2015). Security Debt is the New Technical Debt. Now Secure [online] Available at: https://www.nowsecure.com/blog/2015/10/08/security-debt-is-the-new-technicaldebt. Accessed on June,2021

Harrison, V., Pagliery, P. (2015). Nearly 1 million new malware threats released every day. CNN Business, 14 April, 2015 [online] Available at: https://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/index.html. Accessed on July, 2021

Cyber security trends in 2021 [Online] Available at : https://purplesec.us/cyber-security-trends-2021. Accessed on May,2021

Kenya Cybersecurity report, (2015),p.9. [Online] Available at: https://www.serianu.com/downloads/KenyaCyberSecurityReport2015. Accessed on June, 2021

Herley C. Why do nigerian scammers say they are from Nigeria 2012[Online] Available at: https://www.thejournal.ie/nigerian-scammers-ay-they-are-from-nigeria-495001-Jun2012. Accessed on April, 2021

Keepnet Labs report,(2020) [online] Available at: https://www.keepnetlabs.com/2020-phishing-trends-report. Accessed on July,2021

Cyberoam report, 2016 [online] Available at: https://www.annualreports.com/HostedData/AnnualReportArchive/s/LSE_SOPH_2016. Accessed on February, 2021

Camino Kavanagh, new-tech-new-threats-and-new-governance-challenges 2019[Online] Available at: https://carnegieendowment.org/2019/08/28/new-tech-new-threats-and-new-governance-challenges-opportunity-to-craft-smarter-responses .Accessed on July, 2021

United Nations report on Cybercrime 2013[Online] Available at: https://www.unodc.org/documents/organized Crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213. Accessed on June, 2021

Accredited University 2018[online] Available at: https://victormatara.com/list-of-accredited-universities-in-kenya-2018. Accessed on July, 2021

APPENDICES

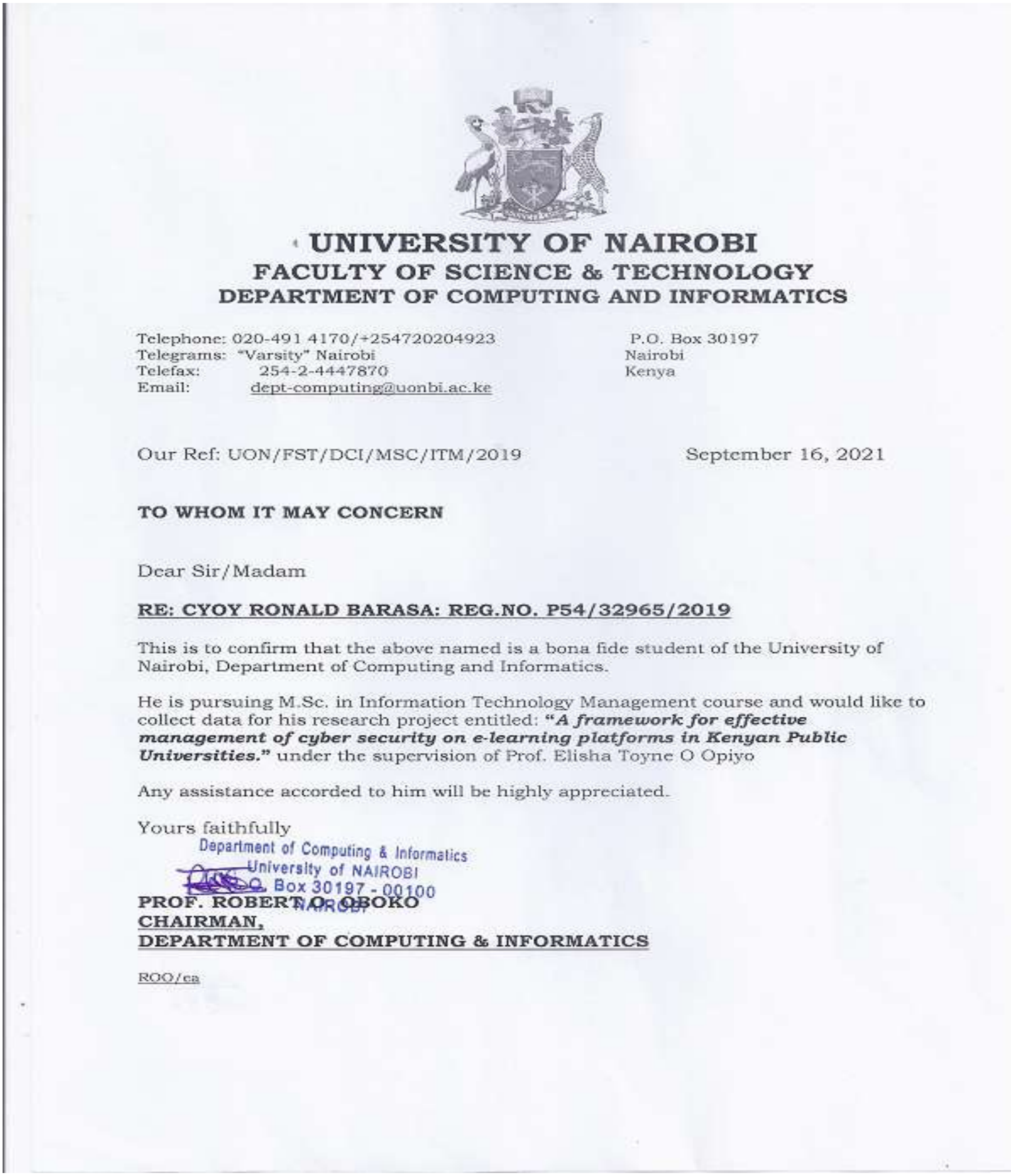
APPENDIX 1. PUBLIC CHARTERED UNIVERSITIES

	Public Chartered Universities	**Year Established/ Accredited**
1.	University of Nairobi	1970
2.	Moi University	1984
3.	Kenyatta University	1985
4.	Egerton University	1987
5.	Jomo Kenyatta University of Agriculture and Technology	1994
6.	Maseno University	2001
7.	Masinde Muliro University of Science and Technology	2007
8.	Dedan Kimathi University of Technology	2012
9.	Chuka University	2013
10.	Technical University of Kenya	2013
11.	Technical University of Mombasa	2013
12.	Pwani University	2013
13.	Kisii University	2013
14.	University of Eldoret	2013
15.	Maasai Mara University	2013
16.	Jaramogi Oginga Odinga University of Science and Technology	2013
17.	Laikipia University	2013
18.	South Eastern Kenya University	2013

19.	Meru University of Science and Technology	2013
20.	Multimedia University of Kenya	2013
21.	University of Kabianga	2013
22.	Karatina University	2013
23.	Kibabii University	2015
24.	Rongo University	2016
25.	The Co-operative University of Kenya	2016
26.	Taita Taveta University	2016
27.	Murang’a University of Technology	2016
28.	University of Embu	2016
29.	Machakos University	2016
30.	Kirinyaga University	2016
31.	Garissa University	2017

Source: Commission for University Education: 2017-2018 University Statistics report

APPENDIX 2: INTRODUCTORY LETTER FOR RESEARCH



UNIVERSITY OF NAIROBI
FACULTY OF SCIENCE & TECHNOLOGY
DEPARTMENT OF COMPUTING AND INFORMATICS

Telephone: 020-491 4170/+254720204923
Telegrams: "Varsity" Nairobi
Telefax: 254-2-4447870
Email: dept-computing@uonbi.ac.ke

P.O. Box 30197
Nairobi
Kenya

Our Ref: UON/FST/DCI/MSC/ITM/2019

September 16, 2021

TO WHOM IT MAY CONCERN

Dear Sir/Madam

RE: CYOY RONALD BARASA: REG.NO. P54/32965/2019

This is to confirm that the above named is a bona fide student of the University of Nairobi, Department of Computing and Informatics.

He is pursuing M.Sc. in Information Technology Management course and would like to collect data for his research project entitled: ***"A framework for effective management of cyber security on e-learning platforms in Kenyan Public Universities."*** under the supervision of Prof. Elisha Toyne O Opiyo

Any assistance accorded to him will be highly appreciated.

Yours faithfully

Department of Computing & Informatics
University of NAIROBI
P.O. Box 30197 - 00100
NAIROBI

PROF. ROBERT O. OBOKO
CHAIRMAN,
DEPARTMENT OF COMPUTING & INFORMATICS

ROO/ea

APPENDIX 3: COVER LETTER

Dear Respondent

RE: VOLUNTARY INVOLVEMENT IN ACADEMIC RESEARCH

Iam a postgraduate student conducting a study on **effective management of cybersecurity on elearning platforms**. This survey aims to seek opinions from various individuals using elearning platforms in the institution. The survey will only take utmost 12 minutes of your time.

Your participation in this academic research is highly appreciated. I take this opportunity to re-assure you that the information provided will be used exclusively for intended research purpose and that confidentiality of information given will be earnestly safeguarded.

Ronald Cyoy
Department of Computing & Informatics
University of Nairobi

APPENDIX 4. QUESTIONNAIRE SURVEY

This questionnaire is purely for academic purpose and is designed to get your opinion on effective management of cyber security on e-learning platforms at your institution, check inside the brackets or box most applicable to you or your institution. Please answer the questions precisely and honestly as possible. Note: All responses will be treated with utmost confidentiality.

SECTION A:

Background information questionnaire

1) Indicate your age

i) 19-23 ( )

ii) 24-29 ( )

iii) 30-34 ( )

iv) 35-39 ( )

v) 40-44 ( )

vi) 45-49 ( )

vii) 50-54 ( )

viii) 55 and over ( )

2) Position held, tick the relevant one for you

i) Student ( )

ii) Administration ( )

iii) Lecturer ( )

3) How is cyber security managed on e-learning platforms at your institution?

i) By vendors ( )

ii) In-house by the IT expert who is tasked a secondary role ( )

iii) In-house computer emergency Response Team ( )

iv) Outsourced to an independent specialized or organization ( )

v) Not sure ( )

4) What cybercrime are prevalent on your e-learning platforms?

i) Hacking ( )

ii) Viruses ( )

iii) Theft of data ( )

5) What security testing techniques are used on e-learning platforms at your university?

i) Vulnerability assessment ( )

ii) Penetration Testing ( )

iii) Audits ( )

iv) Don’t Know ( )

6) Are trainings and awareness done in the institution to manage cyber security, if so how often?

i) Weekly basis ( )

ii) Monthly basis ( )

iii) Yearly basis ( )

iv) Never ( )

7) Does your institution host its own Servers or it is vendor based Services?

i) Servers ( )

ii) Vendor Based ( )

8) What e-learning platforms does your institution use for teaching?

A - Google Class () B - Zoom for Education ( ) C - Moodle ( ) D - Don’t Know ()

SECTION B

Kindly provide your response by checking inside the box most applicable to elearning platforms at in your institution

1) Please indicate how identity facility affects effective management of cyber security on e-learning platforms at your institution.

   Use the scale from Strongly Disagree (SD) to Strongly Agree (SA), by ticking in the appropriate box. (Strongly Disagree (SD), Disagree (D), Neutral (N), Agree (A) and Strongly Agree (SA)

	Identity facility on effective management of cyber security on e-learning platforms	SD	D	N	A	SA
1.	Does the e-learning platform at your university have an identity facility					
2.	Does the identity facility have alerts for threats					
3.	Does the identity facility have authorization levels for the different categories of users					

2) Please indicate how protection affects effective management of cyber security on e-learning platforms in your institution

	Protection facility on effective management of cyber security on e-learning platforms	SD	D	N	A	SA
1.	Does the e-learning platform at your university have a protection facility?					
2.	Does the protection facility provide for login password verification					
3.	Does the protection facility have antivirus and or firewalls security features					

3) Please indicate how Detection affects effective management of cyber security on e-learning platforms in your institution.

	Detection facility on effective management of cyber security on e-learning platforms	SD	D	N	A	SA
1.	Does the e-learning platforms at your university have Detection facility?					
2.	Does the Detection facility on e-learning platforms have capability to check anomalies and report events					
3.	Does the detection facility have inbuilt cyber security corrective processes					

4) Please indicate how response affects effective management of cyber security on e-learning platforms at your institution.

	Response facility on effective management of cyber security on e-learning platforms	SD	D	N	A	SA
1.	Do e-learning platforms have incident Response planning facility when threats are detected or occur					
2.	Does the response facility allow for efficient incidence turnaround time					
3.	Does the response facility have an in built cyber security audit logs reporting system					

5) Please indicate your level of agreement on effective cyber security management on e-learning platforms at your institution

	Indicate levels of your agreement on effective cyber security management on e-learning platforms at your institution	SD	D	N	A	SA

1.	Does the e-learning platforms at your institution provide for effective data system integrity					

6) Please indicate how User compliance affects effective management of cyber security on e-learning platforms at your institution.

	Indicate how user compliance and User skills affects effective management of elearning platforms at your institution	SD	D	N	A	SA
1.	Does user compliance affect management of cyber security on e-learning platform					
2.	Do user skills affects management of cyber security on e-learning platforms at your institution					

Thank you for your response