EXPLORING THE ROLE OF CYBER SECURITY THREAT AWARENESS ON CREATION OF A SECURE LEARNING ENVIRONMENT IN KENYA'S TERTIARY INSTITUTIONS: A CASE OF NAKURU COUNTY

Shadrack Toroitich Lomatong

19s01dmgp007

A THESIS SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTER OF GOVERNANCE PEACE AND SECURITY STUDIES IN THE DEPARTMENT OF GOVERNANCE PEACE AND SECURITY STUDIES OF AFRICA NAZARENE UNIVERSITY

July 2026

DECLARATION

This research is my original work and has not been presented before to any university for academic award.

Signature:  Date: 01 July 2026

SHADRACK TOROITICH

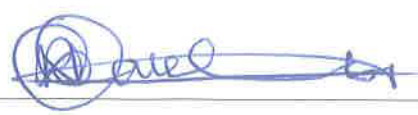
REG NO. 19S01DMGP007

Declaration by the University Supervisors

This research was conducted under our supervision and is submitted under our approval as University Supervisors.

Signature:  Date: 01 July 2026

Dr. ISRAEL NYABURI NYADERA

Signature:  Date: 02 July 2026

Dr. RAPHAEL OGUTU

DEDICATION

To Almighty God who is always there when I am in need. Thank you for giving me strength in my everyday life. I also dedicate this research to my family.

ACKNOWLEDGEMENT

I would like to express my heartfelt gratitude to my supervisors, Dr. Israel Nyaburi Nyadera and Dr. Raphael Ogutu, for their invaluable guidance, patience, and support throughout this research. Their insightful feedback and encouragement have been instrumental in shaping this study. I am also deeply thankful to my classmates for their camaraderie, thought-provoking discussions, and unwavering support, which have enriched my academic journey. Special appreciation goes to my family, whose constant love, prayers, and encouragement provided the motivation and strength needed to complete this work. Finally, I extend my gratitude to all the respondents and participants in this study for their time and valuable insights, which greatly contributed to the success of this research.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

Cybersecurity threats pose significant risks in today's interconnected world, impacting individuals, organizations, and national security. Despite the growing incidence of cyberattacks on private and public institutions, limited attention has been given to individual cybersecurity awareness, particularly in developing countries. This study examines cybersecurity threat awareness among students in tertiary institutions in Nakuru County, Kenya, focusing on their knowledge of cybersecurity policies, experiences with cyber threats, and institutional preparedness. Guided by the Social Learning Theory and Technology Acceptance Model, the study adopts a convergence explanatory research design. The target population comprises 43,500 students, with a sample size of 396 selected using Yamane's formula. Data was collected through questionnaires, interviews, and focus group discussions, and analyzed using thematic and statistical techniques. The findings reveal a moderate awareness of cybersecurity policies among students, with significant knowledge gaps that expose them to risks. A substantial number have encountered cybersecurity threats, including phishing, malware attacks, and social engineering scams, highlighting the need for targeted educational interventions. Institutional preparedness plays a crucial role in fostering a secure learning environment; however, many institutions lack adequate cybersecurity infrastructure and training programs. Correlation analysis indicated strong positive relationships between key variables: awareness of cybersecurity policies and creation of a secure learning environment ($r = 0.851$; $p = 0.000$), incidence of cybersecurity threats and secure learning environments ($r = 0.863$; $p = 0.000$), access to cybersecurity education and creation of a secure learning environment ($r = 0.816$; $p = 0.000$), and institutional preparedness and secure learning environments ($r = 0.848$; $p = 0.000$), Regression results showed that Extent of Awareness of Cybersecurity Policies ($\beta = 0.257$; $p = 0.000$), Incidence of Cyber Security Threats Experienced ($\beta = 0.310$; $p = 0.000$), Preparedness of Diverse Tertiary Institutions ($\beta = 0.228$; $p = 0.000$), and Access to Cybersecurity Education ($\beta = 0.176$; $p = 0.000$) were significant predictors of the creation of a secure learning environment. The overall model was highly significant ($R = 0.899$; $R^2 = 0.808$; $F(4,336) = 354.555$; $p < 0.001$). Based on these findings, the study recommends integrating comprehensive cybersecurity awareness programs into tertiary curricula, enhancing institutional cybersecurity policies and infrastructures, and offering continuous training to strengthen students' resilience to cyber threats. Additionally, policymakers and educational stakeholders should support the development of robust cybersecurity frameworks to safeguard learning environments. Universities should establish cybersecurity task forces, collaborate with industry experts, and ensure that all students, irrespective of the type of institution attended, have equal access to cybersecurity education and protection mechanisms. Future research should assess the long-term effectiveness of cybersecurity interventions and explore the role of emerging technologies in mitigating cyber risks within academic settings.

OPERATIONAL DEFINITION OF TERMS

Kenya's Tertiary Institutions: Kenya's tertiary institutions refer to all higher education institutions offering post-secondary education, including universities, colleges, and technical and vocational education and training (TVET) institutions, located within the geographic area of Nakuru County.

Cybersecurity Policies: Cybersecurity policies refer to the formal regulations, guidelines, and protocols established to govern the use, protection, and management of digital resources and information systems. These policies may include rules regarding data privacy, network security, acceptable use of technology, incident reporting procedures, and compliance with national or international cyber security standards.

Common Cyber Threats: Common cyber threats refers to the prevalent risks and vulnerabilities faced by individuals and organizations operating in digital environments, including but not limited to phishing attacks, malware infections, social engineering scams, ransom ware, identity theft, data breaches, and unauthorized access to sensitive information.

Incidence of Cyber Security Threats: Incidence of cyber security threats pertains to the frequency and severity of cyber-attacks, breaches, or security incidents experienced by students within the tertiary institutions

under study. This includes both successful and attempted cyber intrusions, unauthorized access to information systems, data breaches, malware infections, and other forms of cyber threats.

Cyber Security Threat Awareness: Cyber security threat awareness refers to students' knowledge, understanding, and consciousness of the various cyber risks, threats, and vulnerabilities affecting digital environments. It encompasses the ability to recognize potential security threats, understand their implications, and adopt proactive measures to mitigate risks and protect against cyber-attacks.

Level of Cyber Security Threat Awareness: The level of cyber security threat awareness quantifies the degree or extent to which students in Kenya's tertiary institutions, particularly within Nakuru County, possess comprehensive knowledge and awareness of cyber security threats, including their nature, prevalence, impact, and preventive measures. This may be assessed based on indicators such as students' ability to identify common cyber threats, understand preventive strategies, and recognize warning signs of potential security breaches.

LIST OF ABBREVIATIONS AND ACRONYMS

CA	Communications Authority of Kenya
COVID-19	Coronavirus Disease 2019
DOS	Denial of Service
KNEC	Kenya National Examinations Council
SPSS	Statistical Package for Social Sciences
SQL	Structured Query Language
TAT	Technology Acceptance Theory
UK	United Kingdom
USA	United States of America

CHAPTER ONE

INTRODUCTION

1.1 Introduction

Cybersecurity threats have become a pervasive concern in educational settings, necessitating a comprehensive understanding of their implications on the learning environment. This chapter provides an overview of the study, highlighting the background, problem statement, and purpose. The chapter also comprises specific objectives, research questions, and the significance of the study, scope of the study, delimitations, limitations, assumptions, conceptual framework, and the theoretical framework.

1.2 Background to the Study

Cybersecurity has become an indispensable aspect of modern society, given the increasing reliance on digital technologies. Tertiary institutions (universities, colleges, and vocational schools) serve as hubs of knowledge and innovation. They are fertile grounds for intellectual growth, but they are also vulnerable to cyber risks (Cardwell, 2024). Students, often immersed in academic pursuits and social interactions, may unwittingly expose themselves to cyber threats due to a lack of awareness. Despite extensive research focusing on cybersecurity threats at the national and organizational levels, there exists a noticeable gap in understanding the awareness and susceptibility of tertiary institution students to such threats (Alqahtani, 2022).

Hackers and organized cybercrime gangs have become considerably more numerous. These criminals have been utilizing innovative techniques to commit cybercrimes. Financial gain from collecting confidential data and holding it hostage is the main driving

force behind hacking. Selling confidential information to rivals on the dark web is another way for hackers to generate money. This practice puts businesses and their clients at serious danger and contaminates cyberspace. As a result, cyberattacks are now a major danger to both the economy and international security. They target vital infrastructure, have a negative financial impact on corporate performance, and result in a large loss of intellectual property (Li & Liu, 2021).

Globally, within the realm of tertiary education, students face unique challenges ranging from academic pressures to social dynamics, all of which intersect with the digital landscape (Gkrimpizi, Peristeras & Magnisalis, 2023). The proliferation of cyber threats, including but not limited to femicide, exam cheating, social media abuses, recruitment into extremist groups via social platforms, extortion, and hacking, poses significant risks to the safety, security, and academic integrity of students (Jones, 2023). However, there is a dearth of comprehensive studies exploring the extent of awareness among students regarding cybersecurity policies, their understanding of threats, and the prevalence of victimization within tertiary institutions.

Studies have revealed that students in both the USA and UK generally have some level of awareness regarding cyber security threats (Daengsi, Pornpongtechavanich & Wuttidittachotti, 2022). However, there are significant discrepancies in the depth of understanding and preparedness between different demographic groups and educational institutions. Nevertheless, both countries have made efforts to integrate cyber security education into school curricula, but the effectiveness of these initiatives varies. Some institutions offer dedicated courses or workshops on cyber security awareness, while others incorporate it into existing IT or computing programs (Al Shabibi & Al-Suqri, 2023).

Many students lack awareness of cybersecurity best practices, leading to inadvertent data breaches. In today's increasingly technology-driven world, fostering awareness is paramount to navigating the evolving role of technology in shaping various aspects of our lives. Students continue to underestimate the severity of cyber threats such as phishing and computer viruses (Alharbi &Tassaddiq, 2023). Using the example of the Silicon Valley in California, USA, Moallem (2019) found that, despite their belief that they are observed when using the Internet and that their data is not secure even on university systems, are not very aware of how to protect their data (Bordonaba-Juste, Lucia-Palacios &Pérez-López, 2020). Also, it appears that educational institutions do not have an active approach to improve awareness among college students to increase their knowledge on these issues and how to protect themselves from potential cyber-attacks, such as identity theft or ransomware (Moallem, 2019).

Cyber security awareness among students in China has been gaining attention, especially with the rapid digitization and internet penetration in the country (Wang, 2022). The Chinese government has been implementing policies to strengthen cyber security education in schools and universities (KPMG China, 2016). Additionally, there are various initiatives by educational institutions and industry bodies to promote cyber security awareness among students. Students in Tertiary institutions in Malaysia and India lack proper cybersecurity awareness and a need of awareness program is needed to increase the level of awareness and minimize successful cyber- attacks (Zulkifli, *et al.,* 2020).

Low cyber security threat awareness among students in South Africa is indeed a concerning issue (Adegoke, *et al.,* 2022). One contributing factor could be the lack of comprehensive cyber security education programs in schools and universities. Without proper education

on cyber threats, students may not recognize the importance of safeguarding their digital information (Mtambeka *et. al.,* 2023). While technology access is increasing in South Africa, not all students have equal access to devices or internet connectivity. In Nigeria, there is not any approach in place to increase the level of cybersecurity awareness to students at colleges and universities, the results also show that students lack the basic knowledge of cybersecurity. There is thus, urgent need to conduct a cybersecurity awareness program and to also include it as a core course at the university level in Nigeria (Gabra, *et al.,* 2022).

This study aims to bridge this gap by delving into the level of cyber threat awareness among students in tertiary institutions. By understanding the students' knowledge, attitudes, and experiences concerning cybersecurity, policymakers, educators, and cybersecurity professionals can devise targeted interventions to mitigate risks and safeguard the well-being of students within educational environments.

Carrying out a study on the level of cyber security threat awareness among students in Kenya's tertiary institutions is imperative due to several pressing situations and publications highlighting the vulnerability of this demographic to cyber threats. For instance, a report published by the Communications Authority of Kenya (CA) in 2022 revealed a significant increase in cybercrime cases targeting tertiary institution students, ranging from phishing attacks to social engineering scams. The report indicated that many students lacked adequate awareness of cyber security protocols, making them easy targets for malicious actors operating online (Communications Authority of Kenya, 2022.

According to Alawida et al. (2022), Students now face extra cyber dangers as a result of the widespread use of digital learning systems in response to the COVID-19 epidemic. Students are more vulnerable to online risks including identity theft, academic fraud, and data breaches as a result of the shift to online classrooms and exams. A study conducted by the Kenya National Examinations Council (KNEC) in 2023 found that a concerning number of tertiary institution students had engaged in academic dishonesty by sharing exam materials through unauthorized online channels, highlighting the need for increased cyber security awareness and vigilance among students (KNEC, 2023).

In addition to academic fraud, students in Kenya's tertiary institutions face a range of other cyber threats, including online harassment, financial scams, and recruitment by extremist groups through social media platforms. A study by Kaibiru, *et al.* (2023) in Kenya documented several cases of students falling victim to online recruitment tactics employed by extremist organizations, underscoring the urgent need for comprehensive cyber security education and awareness initiatives within tertiary institutions. These studies have not looked at the role of cyber security threat awareness on creation of a secure learning environment in Kenya’s tertiary institutions.

1.3 Statement of the Problem

Cybersecurity threats in tertiary institutions have become a pressing global concern, with students increasingly targeted by phishing scams, identity theft, ransomware, and cyberbullying (Mensah & Asante, 2023; Tan & Lim, 2021). In developed nations such as the United States and the United Kingdom, significant investments in cybersecurity education, institutional policies, and awareness programs have improved students' ability

to recognize and mitigate cyber risks (Al Shabibi & Al-Suqri, 2023). However, in many developing countries, including Kenya, cybersecurity awareness remains low, leaving students and educational institutions highly vulnerable to cyber threats (Gabra et al., 2022). Kenya's tertiary institutions face escalating cybersecurity challenges due to increased internet penetration, reliance on digital platforms for academic purposes, and the growing sophistication of cybercriminals (Communications Authority of Kenya, 2022). Reports indicate that students frequently fall victim to financial fraud, social engineering attacks, and online recruitment by extremist groups (KNEC, 2023). The COVID-19 pandemic further intensified these vulnerabilities as institutions transitioned to remote learning, exposing students to new digital risks such as exam malpractices facilitated through unauthorized online platforms (Alawida et al., 2022). Despite these concerns, cybersecurity awareness programs remain underdeveloped, and institutions lack comprehensive policies to equip students with essential cybersecurity knowledge and protective measures. While global studies highlight the effectiveness of cybersecurity education in reducing cybercrime risks among students, there is a notable research gap in the Kenyan context. Existing literature in Kenya primarily focuses on national cybersecurity strategies and organizational responses to cyber threats, with limited empirical research on individual awareness levels among students in tertiary institutions. This gap in knowledge hinders the formulation of targeted policies that address students' unique cybersecurity challenges. Without an in-depth understanding of students' awareness, experiences, and institutional preparedness, efforts to secure learning environments remain inadequate. This study seeks to bridge this gap by assessing cybersecurity threat awareness among students in Nakuru County's tertiary institutions. It will examine students' knowledge of cybersecurity policies,

experiences with cyber threats, and the preparedness of institutions to mitigate risks. Addressing these issues is critical to enhancing cybersecurity education, informing institutional policy reforms, and ultimately ensuring a safer learning environment for students in Kenya.

1.4 Purpose of the Study

The purpose of this study was to explore the role of cyber security threat awareness on creation of a secure learning environment in Kenya's tertiary institutions within Nakuru County.

1.5 Objectives of the Study

The objectives of the study include:

i. To determine the extent to which students in Nakuru County's tertiary institutions are aware of cyber security policies and their implication on secure learning environment.
ii. To investigate incidences of cyber security threats experienced by students in Nakuru County's tertiary institutions and their implication on secure learning environment.
iii. To assess the preparedness of diverse tertiary institutions in Nakuru County to counter cyber security threats and their implication on secure learning environment.

1.6 Research Questions

To achieve the aforementioned objectives, the following research questions guided the study:

i. What is the extent of awareness among students in Nakuru County's tertiary institutions regarding cyber security policies and their implication on secure learning environment?
ii. What are the incidences of cyber security threats experienced by students in Nakuru County's tertiary institutions and their implication on secure learning environment?
iii. How prepared are diverse tertiary institutions in Nakuru County to counter cyber security threats and their implication on secure learning environment?

1.7 Significance of the Study

This study holds significant importance for various stakeholders, including policymakers, educators, cybersecurity professionals, and tertiary institution administrators. Understanding the extent of students' awareness of cyber security policies will inform the development of more effective and targeted policies at both national and institutional levels. Policymakers will use the findings to shape legislation and regulations that promote cyber security education and awareness initiatives in tertiary institutions.

Educators will use the findings to tailor their curriculum and teaching methods to better address cyber security issues. By knowing the level of awareness among students, educators will be able develop and deliver more relevant and impactful cyber security education programs. The insights gained from the research can help cybersecurity

professionals identify areas where additional training or resources may be needed. They can also use the findings to collaborate with educational institutions to develop specialized training programs or workshops to enhance students' cyber security skills.

Tertiary Institution Administrators will use the findings to assess the effectiveness of existing cyber security measures within their institutions. This information will guide them in implementing improvements or adjustments to policies and procedures to better protect students and institutional assets from cyber threats. By shedding light on the level of cyber threat awareness among students in tertiary institutions, the findings of this study – are intended to inform the development and implementation of targeted interventions aimed at enhancing cybersecurity measures within educational environments.

Additionally, the study's findings will contribute to the body of knowledge on cybersecurity in educational settings, thereby filling a crucial gap in existing literature. Furthermore, by understanding students' experiences and perceptions of cyber threats, policymakers and educators will design educational programs to promote cyber literacy and resilience among students, equipping them with the necessary skills to navigate the digital landscape safely and securely.

1.8 Scope of the Study

The scope of this study is limited to assessing the level of cyber security threat awareness among students in tertiary institutions in Nakuru County, Kenya. Nakuru County is selected as the study location due to its representative nature as one of the key urban centers in Kenya, hosting several tertiary institutions, including universities, colleges, and

vocational schools. The study will focus on Kabarak University - Nakuru Town Campus, African Institute of Research and Development Studies - Nakuru Town Campus, Mount Kenya University, Institute of Advanced Technology - Nakuru Campus, Kenya Institute of Development Studies - Naivasha Campus (Oserian Estate), Kenya Medical Training College - Nakuru Campus and Kenya Wildlife Service Training Institute - Main campus (See Appendix IV). The study will focus on students enrolled in various tertiary institutions within Nakuru County, encompassing both public and private educational institutions. The target population will include undergraduate and postgraduate students across diverse fields of study. Specifically, the study will investigate the extent to which students are aware of cyber security policies implemented nationally and within their respective institutions, their understanding of common cyber threats prevalent in Nakuru County's tertiary institutions, the incidence of cyber security threats experienced by students, and their knowledge of peers who have fallen victim to such threats.

The rationale for this study lies in the critical need to understand and address cyber security challenges within tertiary institutions in Nakuru County. By focusing on undergraduate and postgraduate students across diverse fields of study in both public and private institutions, the research aims to provide comprehensive insights into the awareness levels, experiences, and attitudes towards cyber security among this demographic. Specifically, investigating students' awareness of national and institutional cyber security policies, their understanding of prevalent cyber threats in Nakuru County's tertiary institutions, and their experiences with cyber security incidents can inform the development of targeted interventions and policies aimed at enhancing cyber security measures within educational environments. Additionally, understanding students' knowledge of peers affected by cyber

threats can shed light on the social dynamics surrounding cyber security awareness and resilience. Ultimately, the findings of this study can serve as a valuable resource for policymakers, educators, cyber security professionals, and tertiary institution administrators in improving cyber security preparedness and resilience within Nakuru County's tertiary institutions.

While the study will provide insights into the general awareness levels among students, it will not delve into specific technical aspects of cyber security or conduct an in-depth analysis of cyber security policies and practices within individual tertiary institutions. Instead, the focus will be on assessing students' perceptions, attitudes, and experiences related to cyber security threats and awareness initiatives. Due to resource constraints and the need for focused research, the study will not extend beyond Nakuru County or include tertiary institutions located in other regions of Kenya.

By delineating the scope in this manner, the study aims to provide a comprehensive understanding of the level of cyber security threat awareness among students in Nakuru County's tertiary institutions, thereby contributing to the development of targeted interventions and policies to enhance cyber security education and resilience within the local educational landscape. The study was carried out across six months, starting from 2024.

1.9 Delimitations

The study focused specifically on tertiary institutions within Nakuru County, Kenya. While this geographic scope provided valuable insights into cybersecurity challenges within a

specific region, the findings may not be directly generalizable to other regions or countries. The study targeted undergraduate and postgraduate students enrolled in tertiary institutions within Nakuru County. Although this population represented a significant demographic in the educational landscape, the findings may not have fully captured the perspectives of other stakeholders, such as faculty, staff, or administrators.

The study examined cybersecurity awareness, experiences, and attitudes among students within a specific time frame, which may have limited the generalizability of the findings to different periods with potentially evolving cybersecurity threats and policies. The study primarily investigated students' awareness of cybersecurity policies, understanding of common cyber threats, experiences with cybersecurity incidents, and knowledge of peers affected by such threats. While these aspects provided valuable insights, other factors such as institutional cybersecurity infrastructure or external influences may also have impacted cybersecurity preparedness.

The study employed quantitative methods to collect and analyze data, which limited the depth of qualitative insights into students' perceptions and experiences with cybersecurity. Additionally, the study's reliance on self-reported data may have introduced response biases and limitations in the accuracy of the reported experiences.

1.10 Limitations

While every effort was made to ensure the validity and reliability of the study's findings, several limitations were inherent in the research design: There was a likelihood of sampling bias if the study relied solely on convenient sampling methods, potentially

leading to a non-representative sample of students. To mitigate this limitation, the researcher employed stratified random sampling techniques in sample identification and purposive sampling techniques in sample selection. By dividing the population of students into relevant strata based on factors such as academic discipline, institution type (public/private), and academic year, the researcher ensured that each subgroup was adequately represented in the sample. This approach helped reduce the risk of sampling bias and improved the generalizability of the study's findings.

There was also a possibility of self-report bias, where participants may have provided inaccurate or biased responses to survey questions related to their awareness of cybersecurity threats due to social desirability or memory recall issues. To address self-report bias, the researcher utilized multiple methods of data collection, including surveys, interviews, and focus group discussions. By triangulating data from different sources, the researcher cross-validated responses and identified any discrepancies or inconsistencies. Additionally, the researcher ensured anonymity and confidentiality in data collection procedures to encourage honest and candid responses from participants.

The findings of the study may have lacked external validity if they were not generalizable to other regions or contexts beyond Nakuru County, Kenya. This limitation could have restricted the applicability of the study's conclusions to broader populations or settings. To enhance the external validity of the study, the researcher provided a detailed description of the study methodology, including sampling procedures, data collection instruments, and analytical techniques. Additionally, the researcher encouraged transparency and reproducibility by sharing raw data and research protocols with other scholars or researchers interested in replicating the study in different geographic locations or

educational contexts. By promoting transparency and rigor in research methods, the researcher increased the likelihood that the study findings would be relevant and applicable beyond the specific context of Nakuru County.

1.11 Assumptions

The study assumed that participants would provide truthful and accurate responses to the research instruments, including questionnaires, interviews, and focus group discussions. This assumption was fundamental for ensuring the reliability and validity of the data collected, as any inaccuracies or biases in participant responses could have compromised the integrity of the findings. Another assumption was that the cybersecurity threat landscape within Kenya's tertiary institutions, particularly in Nakuru County, was representative of broader trends and challenges facing educational environments globally. While the study focused on a specific geographical area, it was assumed that the insights and findings derived from this context would have relevance and applicability to similar educational settings elsewhere.

Additionally, the study assumed that the implementation of effective cybersecurity policies and practices within tertiary institutions could significantly contribute to the creation of a secure learning environment. This assumption underscored the importance of proactive measures and interventions in mitigating cyber threats and safeguarding academic resources, infrastructure, and intellectual property.

1.12 Theoretical Framework

This study is grounded in two key theoretical perspectives: Social Learning Theory and the Technology Acceptance Theory (TAT). These theories provide a comprehensive framework for understanding how students in Kenya's tertiary institutions acquire cybersecurity awareness, perceive cybersecurity policies, and adopt protective behaviors. The integration of these theories allows for a multidimensional analysis of cybersecurity threat awareness, capturing both social influences and individual decision-making processes in the adoption of cybersecurity practices.

1.12.1 Social Learning Theory (SLT)

Social Learning Theory, developed by Albert Bandura (1977), posits that individuals acquire knowledge and behaviors through observation, imitation, and social interactions. According to Bandura, learning does not occur solely through direct experiences but is significantly influenced by observing others, particularly role models such as peers, educators, and institutional leaders. The theory emphasizes three key mechanisms of learning: observational learning, modeling, and reinforcement.

In the context of this study, Social Learning Theory is particularly relevant in explaining how students in tertiary institutions develop awareness and behavioral responses to cybersecurity threats. Students frequently interact with digital platforms, where they observe peers falling victim to cyber threats such as phishing, hacking, and identity theft. Their awareness and willingness to adopt cybersecurity measures may be shaped by witnessing the consequences of cyber incidents on others. For instance, if students observe their classmates experiencing financial loss due to a phishing scam, they may become more

cautious and proactive in identifying similar threats. Conversely, a lack of visible consequences may lead to complacency, reinforcing risky online behaviors.

Moreover, reinforcement plays a crucial role in shaping cybersecurity behaviors. Positive reinforcement, such as institutional recognition for good cybersecurity practices or tangible rewards for safe online behaviors, can encourage students to follow cybersecurity guidelines. On the other hand, negative reinforcement, such as disciplinary action for academic fraud facilitated by cyber threats, can deter students from engaging in risky online activities. Educational institutions can leverage these reinforcement mechanisms by embedding cybersecurity awareness into student engagement programs, academic curricula, and institutional policies.

Social Learning Theory also underscores the importance of institutional influence. If university administrators and lecturers actively promote cybersecurity awareness by modeling safe online behaviors, disseminating knowledge on cyber threats, and enforcing cybersecurity policies, students are more likely to adopt these practices. Conversely, a lack of institutional emphasis on cybersecurity may lead to a culture of negligence, where students remain unaware of potential threats and do not take preventive measures. This study applies SLT to assess how students' cybersecurity awareness is shaped by their social environment, institutional policies, and peer influences within Nakuru County's tertiary institutions.

1.12.2 Technology Acceptance Theory (TAT)

The Technology Acceptance Theory (TAT), proposed by Fred Davis (1989), explains how individuals accept and use technology based on two key factors: perceived usefulness (PU)

and perceived ease of use (PEOU). Perceived usefulness refers to the extent to which an individual believes that using a particular technology will enhance their performance or provide a significant benefit. Perceived ease of use refers to the degree to which an individual finds the technology easy to understand and operate. The combination of these two factors influences an individual's behavioral intention to adopt and use technology effectively.

In the context of cybersecurity awareness among students, TAT provides insights into how students perceive and adopt cybersecurity policies, security software, and safe online behaviors. If students perceive cybersecurity measures as useful—for instance, believing that strong passwords, multi-factor authentication, and antivirus software protect them from cyber threats—they are more likely to adopt these measures. However, if they view cybersecurity measures as complex, time-consuming, or restrictive (low perceived ease of use), they may resist adopting them, even when they acknowledge their importance.

This study applies TAT to assess how students in Nakuru County's tertiary institutions interact with cybersecurity technologies and policies. For example, students might be aware of cybersecurity policies but may not actively adhere to them if they find them difficult to implement. Similarly, students might avoid using complex passwords or updating their software regularly if they perceive these practices as inconvenient. By examining these perceptions, this study will provide insights into the barriers preventing students from fully embracing cybersecurity measures.

Additionally, TAT highlights the role of external variables, such as training and institutional support, in shaping students' acceptance of cybersecurity practices.

Universities that offer structured cybersecurity training sessions and provide user-friendly security solutions can enhance both perceived usefulness and ease of use, encouraging students to adopt protective measures. In contrast, institutions that fail to provide adequate guidance or resources may inadvertently discourage students from prioritizing cybersecurity.

1.12.3 Integration of Social Learning Theory and Technology Acceptance Theory

The combination of SLT and TAT provides a robust theoretical framework for understanding cybersecurity awareness and behavior among students in tertiary institutions. While SLT explains how social interactions and observational learning influence cybersecurity awareness, TAT provides insights into students' decision-making processes regarding the adoption of cybersecurity practices.

This study will examine how students' awareness of cybersecurity policies is shaped by peer interactions and institutional influence (as explained by SLT) while also analyzing how students' willingness to adopt cybersecurity measures is influenced by their perceptions of usefulness and ease of use (as explained by TAT). The interplay of these two theories will provide a comprehensive understanding of the factors driving or hindering cybersecurity awareness and adoption in Nakuru County's tertiary institutions.

By integrating these theoretical perspectives, the study will contribute to the development of targeted interventions aimed at improving cybersecurity education, enhancing institutional cybersecurity policies, and fostering a culture of proactive cybersecurity practices among students. This approach will help bridge the existing gap in cybersecurity

awareness, ensuring that Kenyan tertiary institutions align with global best practices in mitigating cyber threats.

1.13 Conceptual Framework

The conceptual framework for the proposed study is presented in Figure 2.1. The conceptual framework guiding this study is anchored on four key independent variables—Extent of Awareness of Cybersecurity Policies, Incidence of Cyber Security Threats Experienced, Preparedness of Diverse Tertiary Institutions, and Access to Cybersecurity Education—which collectively influence the dependent variable, Creation of a Secure Learning Environment. Each independent variable is broken down into measurable indicators, such as data protection policies, threat encounter frequency, and curriculum integration levels. The framework also incorporates Access to Cybersecurity Education as an intervening variable, recognizing that education and training efforts can mediate the relationship between cybersecurity awareness and the establishment of a secure learning environment. Through this model, the study seeks to examine how students' cybersecurity knowledge, experiences, institutional readiness, and exposure to cybersecurity education interact to promote or hinder the creation of a secure and resilient digital learning atmosphere in Kenya's tertiary institutions.

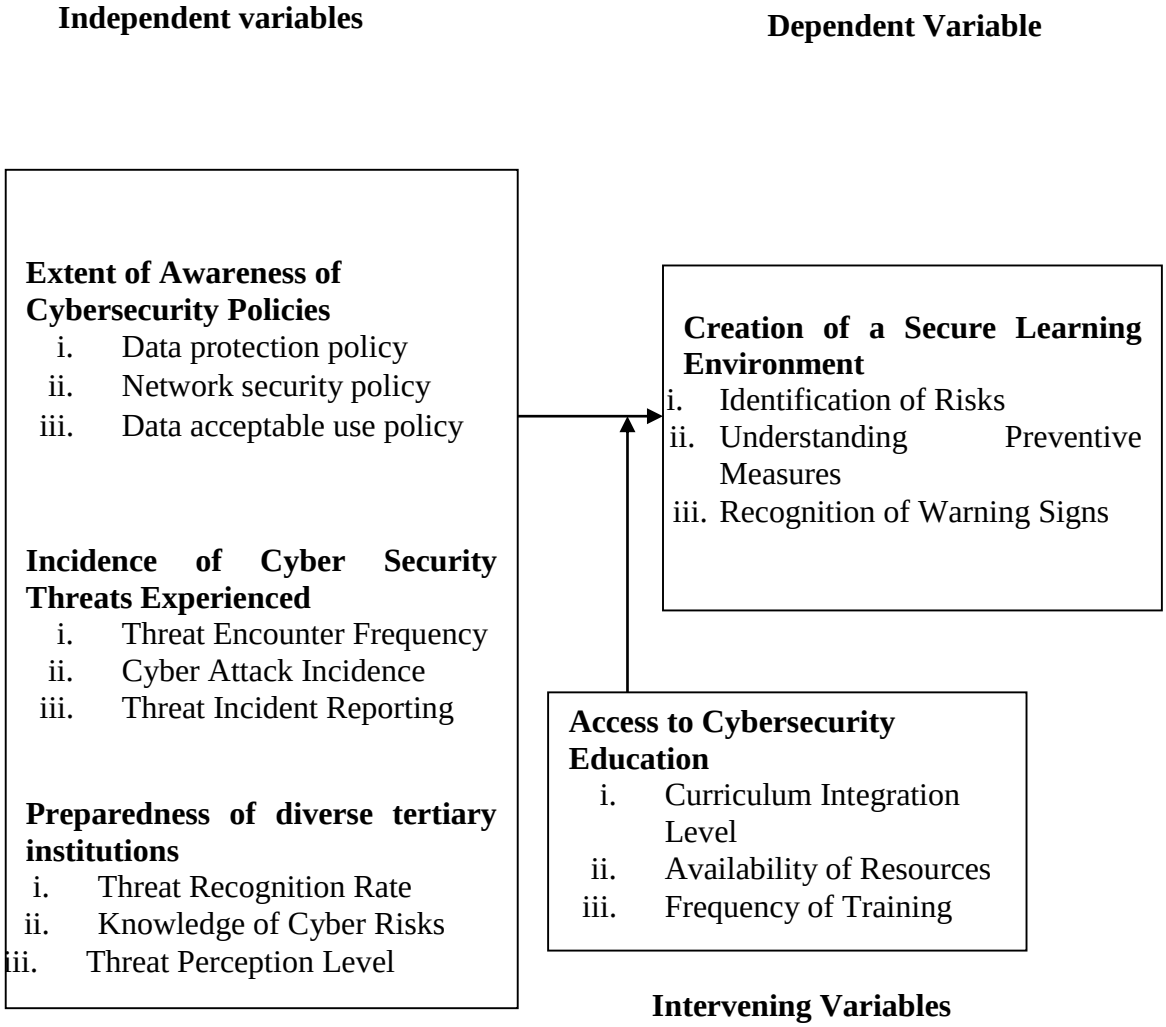


Figure 1. 1: Conceptual Framework Depicting the role of Cyber Security threat awareness on Creation of a Secure Learning Environment

The conceptual framework for this study revolves around three independent variables aimed at assessing different aspects of students' awareness and experiences related to cybersecurity in tertiary institutions in Kenya. The first independent variable focuses on the Extent of Awareness of Cybersecurity Policies, which includes indicators such as students' awareness of data protection policy, network security policy and data acceptable use policy. This variable aims to gauge students' familiarity with and adherence to existing

cybersecurity policies within their educational institutions, providing insights into the effectiveness of institutional cybersecurity measures.

The second independent variable, Students' Awareness of Common Cyber Threats, delves into students' knowledge and recognition of prevalent cyber threats. This variable encompasses indicators like Threat Recognition Rate, Knowledge of Cyber Risks, and Threat Perception Level, which collectively assess students' understanding of potential cybersecurity risks they may encounter. By examining students' awareness of common threats, the study seeks to identify areas where educational interventions on cybersecurity may be needed to enhance students' preparedness.

Lastly, the third independent variable, preparedness of diverse tertiary institutions. This variable includes indicators such as Threat Encounter Frequency, Cyber Attack Incidence, and Threat Incident Reporting, which aim to quantify the prevalence and impact of cyber threats faced by students in tertiary institutions. Understanding the frequency and nature of cyber incidents can inform strategies for improving cybersecurity protocols and response mechanisms within educational settings.

These independent variables collectively contribute to understanding the level of cyber security threat awareness among students in Kenya's tertiary institutions, shedding light on various aspects of policy adherence, threat recognition, personal experiences, and social dynamics within educational environments. Additionally, the framework incorporates an intervening variable, Access to Cybersecurity Education, which highlights the role of educational initiatives and resources in shaping students' cybersecurity awareness and preparedness.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

The literature review section serves as a crucial component of this study, offering a comprehensive synthesis of existing research pertaining to cyber security threat awareness among tertiary institution students in Kenya. This chapter aims to provide a foundation for the study by examining relevant empirical evidence related to the specific objectives outlined in Chapter One.

2.2 Reviewed Literature/Empirical Review

2.2.1 Threat awareness among Students in Tertiary Institutions

Awareness of common cyber threats prevalent in tertiary institutions among students is a critical aspect of ensuring their digital safety and security. Numerous studies conducted across different countries shed light on the extent of students' awareness regarding these threats. In Pakistan, a study by Khan et al. (2022) investigated students' awareness of common cyber threats prevalent in higher education institutions. The results indicated that while students were generally aware of well-known cyber threats such as phishing and malware, there was limited understanding of emerging threats such as social engineering attacks. Additionally, research conducted in Malaysia by Tan and Lim (2021) underscored the importance of proactive cyber security education initiatives in enhancing students' awareness of evolving cyber threats and promoting a culture of cyber hygiene.

Research conducted in various countries provides valuable insights into students' awareness of common cyber threats prevalent in tertiary institutions. In Pakistan, Khan et al. (2022) investigated students' awareness of cyber threats in higher education institutions. The study found that while students demonstrated awareness of well-known threats such as phishing and malware, there was limited understanding of emerging threats like social engineering attacks. This suggests a need for comprehensive cyber security education to enhance students' awareness of evolving cyber threats and promote proactive measures to mitigate risks.

Similarly, research conducted in Malaysia by Tan and Lim (2021) underscored the importance of proactive cyber security education initiatives in tertiary institutions. The study revealed that students possessed varying levels of awareness regarding different cyber threats, with some students lacking knowledge of potential risks such as identity theft and ransomware. This highlights the importance of comprehensive cyber security curriculum to equip students with the necessary knowledge and skills to protect themselves against diverse cyber threats.

The findings from Pakistan in Khan et al. (2022) and Malaysia in (Khan *et al.*, 2022) cannot be directly generalized to Kenya's tertiary institutions due to potential cultural and contextual differences in cyber security awareness. While these studies provide insights into students' awareness of common cyber threats, such as phishing and malware, they may not reflect the specific cyber security landscape in Kenya. Variations in educational systems, technological infrastructure, and socio-cultural factors could influence the prevalence and understanding of cyber threats among Kenyan students. Therefore,

conducting a localized study specific to Kenya's tertiary institutions is necessary to accurately assess students' awareness of cyber threats and tailor interventions accordingly.

In Ghana, Mensah and Asante (2023) examined the prevalence of cyber security threats experienced by students in tertiary institutions. The study identified a range of threats including data breaches, phishing attempts, and online harassment. Despite these risks, many students lacked awareness of cyber security best practices, making them vulnerable to exploitation. This highlights the urgent need for educational institutions to prioritize cyber security awareness initiatives to empower students to safeguard their digital assets and personal information. Similarly, in Nigeria, Adekunle et al. (2020) found that students in tertiary institutions faced various cyber threats, including phishing scams and social media hacking. However, the study revealed gaps in students' awareness of cyber security measures and reporting protocols, indicating a need for enhanced education and training on cyber security awareness and incident response.

However, the findings from Ghana in Mensah and Asante (2023) and Adekunle et al. (2020) in Nigeria may not directly apply to Kenya's tertiary institutions due to differences in cyber security practices and educational contexts. While these studies highlight the prevalence of cyber threats experienced by students, the specific types of threats and levels of awareness may vary across countries. Factors such as internet usage patterns, cyber security policies, and institutional support for cyber security education could differ between Ghana, Nigeria, and Kenya, impacting students' awareness and vulnerability to cyber threats. Therefore, a comprehensive study focusing specifically on Kenya's tertiary institutions is essential to understand the unique cyber security challenges faced by students in the country.

In Kenya, Chizanga, Agola and Rodrigues (2022) found that there is low level of awareness and the university students and staff. A survey tested academic staff from 31 public universities for the variable cyber security awareness, the variable cyber security self-perception, and the factors influencing cyber security awareness. The results shows that a significant number of respondents do not have adequate cyber security training. The study conducted in Kenya by Chizanga, Agola, and Rodrigues (2022) indicates a low level of cyber security awareness among university students and staff. While this study provides valuable insights into the cyber security landscape in Kenya, it focuses primarily on academic staff from public universities. Therefore, the findings may not fully capture the cyber security awareness levels among students in various tertiary institutions across Kenya. Additionally, the study primarily examines the factors influencing cyber security awareness without delving into the specific types of cyber threats prevalent among students. Conducting a broader study encompassing students from diverse tertiary institutions in Kenya would provide a more comprehensive understanding of their awareness of common cyber threats and inform targeted interventions to enhance cyber security education and preparedness.

Building upon these findings, it is evident that students in tertiary institutions possess varying levels of awareness regarding common cyber threats. Comprehensive cyber security education programs are essential to equip students with the knowledge and skills needed to identify, prevent, and respond to cyber threats effectively. By enhancing students' awareness of cyber risks and promoting proactive measures, tertiary institutions can create a safer digital environment for their students and mitigate the potential impact of cyber-attacks on academic pursuits and personal well-being.

2.2.2 The Incidence of Cyber Security Threats Experienced By Students in Tertiary Institutions

The incidence of cyber security threats experienced by students in tertiary institutions is a significant concern that requires careful examination. Several studies conducted across different countries provide insights into the prevalence and nature of these threats. Jawaid (2023) investigated the impact of the COVID-19 pandemic on the incidence of cyber security threats among students in tertiary institutions in the USA. Using longitudinal data collected before and during the pandemic, the study assessed changes in cyber security threat trends and students' perceptions of online security risks. Results indicated a significant increase in cyber security incidents following the transition to remote learning, with students reporting higher rates of phishing attempts, online harassment, and data breaches. Moreover, the study underscored the importance of proactive cyber security measures and institutional support for mitigating the heightened risks associated with remote education environments. There was a lack of clear cybersecurity policies for educational institutes and universities in 2020, according to a report by Microsoft Security Intelligence.

In China, a study by Li and Liu (2020) examined the prevalence and nature of cyber security threats among students in tertiary institutions. Employing a mixed-methods approach, the researchers surveyed students and conducted qualitative interviews to explore their experiences with cyber threats and their perceptions of institutional cyber security measures. The study found that Chinese students reported similar types of cyber security threats as their counterparts in the US, including phishing attacks, data breaches, and malware infections. Additionally, the research identified cultural and institutional

factors that influenced students' cyber security behaviors, such as attitudes towards privacy, technology use norms, and the availability of support resources for cyber security education and training.

In Pakistan, research by Khan et al. (2022) highlighted that students in higher education institutions commonly faced cyber security threats such as phishing attempts, malware infections, and unauthorized access to personal data. The study revealed that a considerable proportion of students had experienced at least one cyber security incident during their academic tenure, underscoring the pervasive nature of cyber threats in tertiary institutions. Similarly, studies conducted in Malaysia by Tan and Lim (2021) indicated that students encountered various cyber security incidents, including data breaches, identity theft, and online harassment. These incidents not only compromised students' personal information and privacy but also disrupted their academic activities and well-being.

In Ghana, research by Mensah and Asante (2023) identified a range of cyber security threats experienced by students in tertiary institutions, including phishing scams, social media hacking, and online fraud. The study found that a significant number of students had fallen victim to cyber-attacks, thus, leading to financial losses, reputational damage, and psychological distress. Similarly, in Nigeria, Adekunle et al. (2020) reported instances of students experiencing cyber security incidents such as email phishing, social media account compromise, and malware infections. These incidents not only affected students' academic performance but also raised concerns about the security of institutional data and systems.

Research conducted in Nigeria provides valuable insights into the incidence of cyber security threats experienced by students in tertiary institutions within the country. Studies

have identified various cyber threats, including phishing scams, social media hacking, and data breaches, affecting students' digital safety and security. However, it's crucial to note that the cyber security landscape in Nigeria may differ from that of other countries due to factors such as internet penetration rates, technological infrastructure, and regulatory frameworks. Therefore, while findings from Nigeria offer insights into the challenges faced by Nigerian students, they may not generalize to other contexts such as Rwanda and Kenya. Conducting separate studies in Rwanda and Kenya is necessary to understand the specific nature and frequency of cyber threats experienced by students in these countries and tailor intervention strategies accordingly.

Research by Ntaganda (2018) conducted in Rwanda sheds light on the incidence of cyber security threats experienced by students in tertiary institutions within the country. Studies have documented various cyber threats, including malware attacks, phishing attempts, and online harassment, impacting students' digital well-being. However, the cyber security landscape in Rwanda may differ from that of Nigeria and Kenya due to unique socio-cultural, technological, and institutional factors. Therefore, while insights from Rwanda provide valuable perspectives on cyber security challenges, they may not directly apply to the context of Kenya and Nigeria. Conducting separate studies in Kenya and Nigeria is essential to capture the distinct challenges and vulnerabilities faced by students in each country and develop tailored strategies to mitigate cyber risks effectively.

In Kenya, research on the incidence of cyber security threats experienced by students in tertiary institutions is crucial for understanding the specific challenges and vulnerabilities within the country. Although previous research conducted in Nigeria by Aliyu et al and Rwanda by Mugisha (2020) provides valuable perspectives, the cyber security

environment in Kenya may exhibit distinct attributes shaped by factors like internet usage trends, technological accessibility, and institutional backing for cyber security initiatives. Therefore, conducting a dedicated study in Kenya is necessary to assess the nature and frequency of cyber threats faced by students and informs the development of targeted intervention strategies tailored to the local context. By examining the experiences of Kenyan students, researchers can identify gaps in cyber security awareness, education, and infrastructure and work towards enhancing students' digital safety and security in tertiary institutions.

These studies highlight the prevalence and impact of cyber security threats on students in tertiary institutions across different countries. The incidence of these threats underscores the urgent need for proactive measures to enhance cyber security awareness, implement robust security protocols, and provide support services to students affected by cyber-attacks. By addressing these challenges, tertiary institutions can create a safer digital environment for their students and promote a culture of cyber security resilience.

2.2.3 Preparedness of Diverse Tertiary Institutions to Counter Cyber Security Threats

In a recent study conducted in the United States by Safitra, Lubis & Fakhrurroja (2023), researchers investigated the preparedness of diverse tertiary institutions to counter cyber security threats through proactive measures and effective response strategies. The study utilized a mixed-methods approach, combining surveys and interviews with cybersecurity professionals across multiple universities. Findings revealed significant variations in the level of preparedness among institutions, with some demonstrating robust cybersecurity infrastructure and policies while others lagged behind. Key factors influencing

preparedness included institutional resources, leadership support, and collaboration with external stakeholders. The study underscored the importance of proactive measures such as regular risk assessments, staff training, and incident response planning in enhancing institutional resilience to cyber threats.

Another study conducted in the US by Cremer (2022) focused on assessing the cyber security preparedness of community colleges, a vital but often overlooked sector of tertiary education. Through surveys and focus group discussions with community college administrators and IT professionals, the study highlighted unique challenges faced by these institutions, including limited financial resources, outdated infrastructure, and lack of dedicated cybersecurity personnel. Despite these challenges, the study identified pockets of innovation and best practices, such as collaborative partnerships with industry partners and participation in cybersecurity training programs. The findings underscored the need for tailored support and resources to strengthen the cyber security posture of community colleges and ensure their resilience against evolving cyber threats.

A study by Cheng and Wang (2022) explored the cyber security preparedness of tertiary institutions in response to emerging threats and challenges in China. Using a qualitative research design, the study examined the effectiveness of proactive measures and response strategies employed by universities across different regions of China. Findings indicated a growing recognition of the importance of cyber security among Chinese tertiary institutions, driven by increasing incidents of cyber-attacks and data breaches. However, the study also identified gaps in preparedness, particularly in areas such as threat intelligence sharing, incident detection, and staff training. Recommendations included strengthening collaboration between academia, industry, and government agencies to

address cybersecurity challenges collectively and enhancing awareness and education initiatives to empower stakeholders with necessary skills and knowledge.

In their study conducted in Pakistan, Saleem, Khan, and Zafar (2021) unearthed a significant correlation between students' awareness of their peers targeted by cyber security threats in tertiary institutions and their understanding of the magnitude and ramifications of such incidents nationwide. Their research shed light on the pivotal role played by peer awareness in shaping perceptions of cyber security risks among students, thereby highlighting the importance of peer-to-peer communication and knowledge-sharing in enhancing cyber security resilience within educational settings. By recognizing the impact of peer experiences on students' perceptions, policymakers and educators can develop targeted interventions to bolster cyber security awareness and response mechanisms, ultimately fostering a safer digital environment for tertiary institution students in Pakistan.

While studies in the UK and USA offer valuable insights, the cyber security landscape in Pakistan may present unique challenges influenced by factors such as internet penetration rates, socio-economic disparities, and regulatory enforcement. Therefore, conducting dedicated research in Pakistan is necessary to assess students' awareness of cyber threats and their experiences with cyber security breaches. By examining the perspectives of Pakistani students, researchers can identify gaps in cyber security education and infrastructure and develop targeted interventions to address emerging threats effectively.

Likewise, in China, research on students' knowledge of peers affected by cyber security threats in tertiary institutions is crucial for assessing the prevalence and consequences of such incidents. While findings from the UK, USA, and Pakistan offer valuable insights,

the cyber security landscape in China may present distinct characteristics shaped by factors such as government censorship, internet regulations, and technological advancements. Therefore, conducting dedicated research in China is necessary to understand students' perceptions of cyber risks and their experiences with cyber security incidents. By examining the perspectives of Chinese students, researchers can identify areas for improvement in cyber security awareness and resilience-building initiatives tailored to the local context.

In a study conducted in Nigeria by Badamasi and Utulu (2021), researchers assessed the cyber security preparedness of tertiary institutions in the country. The study employed a mixed-methods approach, combining surveys and interviews with IT administrators and security personnel from various universities. Findings revealed significant disparities in the level of preparedness among institutions, with some demonstrating robust cyber security measures while others lagged behind. Factors influencing preparedness included budget allocation, access to technical expertise, and institutional commitment to cyber security. Recommendations included the need for increased investment in cyber security infrastructure, regular training for staff and students, and the establishment of collaborative networks for sharing threat intelligence and best practices.

Mugisha (2020) explored the cyber security challenges facing tertiary institutions in Rwanda and their readiness to counter these threats. The research involved surveys and focus group discussions with IT administrators, academic staff, and students from multiple universities. Results indicated a growing awareness of cyber security risks but limited resources and capacity to address them effectively. Challenges included inadequate funding, shortage of skilled personnel, and limited access to up-to-date technology. Even

though, the Government of Rwanda adopted a national cyber security policy in 2015 to help safeguard government information and infrastructure against a growing number of cyber-attacks, the level of preparedness is still very low.

In a recent study by Gabra et al., 2022), the preparedness of diverse tertiary institutions in Kenya to counter cyber security threats was investigated. Through a comprehensive survey and analysis, the researchers found that while some institutions had implemented proactive measures such as cybersecurity awareness programs and regular security audits, there were significant gaps in overall preparedness. Factors contributing to these gaps included limited financial resources, inadequate training for staff and students, and a lack of coordination between IT departments and other stakeholders. The study underscored the need for tertiary institutions to prioritize cyber security investments and develop robust response strategies to mitigate risks effectively.

2.3 Chapter Summary

The empirical review highlights the critical role of cybersecurity awareness policies in shaping students' understanding and preparedness to tackle cyber threats in various global contexts. Research across multiple countries has consistently pointed to gaps in students' awareness of cybersecurity policies, which are influenced by the clarity of policy communication and the accessibility of information. For instance, studies from the United Kingdom by Al Shabibi and Al-Suqri (2023) and the United States by Jones and Brown (2020) showcased that while students may be aware of the existence of these policies, their understanding of specific protocols remains superficial. Similarly, investigations in Pakistan (Khan et al., 2022) and Malaysia (Ariffin & Lim, 2021) found that despite a

general acknowledgment of cybersecurity's importance, significant barriers, including complex policy language and inadequate training, hindered effective awareness. This indicates a shared challenge across institutions, emphasizing the need for improved communication strategies and educational initiatives that transcend geographical borders (Bottyán, 2023; Zhang et al., 2022).

Gaps in the current research on cybersecurity awareness policies from various regions point to the necessity for localized studies that consider the unique socio-cultural and educational contexts of Kenya's tertiary institutions. While findings from countries such as China and Ghana reveal strides made in policy implementation and awareness, they may not be directly applicable to Kenyan institutions due to distinct technological and regulatory landscapes (Mensah & Asante, 2023; Aliyu et al., 2020). The observed disparities underline the importance of understanding local conditions, which can significantly affect how cybersecurity policies are perceived and adhered to by students. Consequently, a targeted investigation into the challenges and facilitators of cybersecurity policy awareness in Kenyan institutions is warranted to inform tailored interventions that resonate with the local demographic.

The review further emphasizes the critical importance of awareness regarding prevalent cyber threats among tertiary students as a foundational component of a secure learning environment. Studies conducted in Pakistan (Khan et al., 2022) and Malaysia (Tan & Lim, 2021) indicate that while students may recognize common threats like phishing, their comprehension of more sophisticated threats, such as social engineering, is lacking. This gap in knowledge points to a pressing need for educational institutions to enhance their curricula with comprehensive cyber threat education that addresses both existing and

emerging risks. Research in Ghana and Nigeria corroborates these findings, revealing that students often remain ill-informed about essential cybersecurity practices, making them vulnerable to exploitation and damage from cyber incidents (Adekunle et al., 2020; Mensah & Asante, 2023).

However, context-specific nuances highlight the necessity of localized studies for accurate assessments of student awareness of cybersecurity threats within Kenya's unique educational infrastructure. Current literature from Ghana and Nigeria illustrates the various threats faced by students but does not sufficiently address Kenya's particularities regarding internet usage patterns and institutional support systems (Wanjiru et al., 2023). Conducting targeted research within Kenya aims to uncover how these factors influence students' awareness and susceptibility to cyber threats, ultimately contributing to the establishment of a safer and more secure digital learning environment in the country's tertiary institutions. Understanding these dynamics will enable stakeholders to implement more effective educational strategies and policies tailored to the specific needs of the Kenyan educational landscape.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

Chapter Three outlines the approach undertaken to assess the level of cyber security threat awareness among students in Kenya's tertiary institutions, with a focus on Nakuru County. This chapter serves as a blueprint for the research process, detailing the methods, techniques, and procedures employed to achieve the study's objectives. This section sets the stage for the discussion, providing an overview of the research methodology adopted.

3.2 Research Design

This study adopted a convergence explanatory research design, which was a type of mixed-methods approach that combined quantitative and qualitative data. The convergence explanatory design allowed for a comprehensive understanding of the research problem by integrating both numerical data analysis and qualitative insights. In adopting a convergence explanatory research design for this study, the aim was to ensure a holistic and in-depth exploration of the role of cyber security threat awareness in creating a secure learning environment in Kenya's tertiary institutions within Nakuru County. By combining quantitative and qualitative data collection methods, this design choice allowed for a multifaceted examination of the research problem. Quantitative data obtained through questionnaires provided numerical measures to assess the extent of cyber security threat awareness among students and institutions, as well as the effectiveness of policy implementation in mitigating security risks. These statistical analyses offered valuable

insights into the prevalence and distribution of cyber security practices, allowing for comparisons and generalizations across different demographic groups within the study population.

On the other hand, qualitative data obtained through interviews offered deeper insights into the underlying mechanisms and contextual factors that influenced cyber security threat awareness and response strategies. Through qualitative analysis, researchers explored the perceptions, attitudes, and experiences of students, educators, and administrators regarding cyber security policies, practices, and incidents. This qualitative lens provided a rich understanding of the social, cultural, and institutional dynamics shaping the cyber security landscape in Nakuru County's tertiary institutions. By integrating both quantitative and qualitative data, the convergence explanatory research design enhanced the validity, reliability, and comprehensiveness of the study findings, allowing for nuanced interpretations and actionable recommendations to enhance cyber security awareness and resilience in the educational context.

3.3 Research Site

The research was conducted in Nakuru County, situated in the central part of the Rift Valley region of Kenya. Geographically, Nakuru County lies approximately 160 kilometers northwest of Nairobi and is bordered by Baringo, Laikipia, Nyandarua, Kericho, Bomet, Kajiado, Narok, and Kiambu counties. Nakuru is one of Kenya’s fastest-growing urban centers and has recently been elevated to city status, reflecting its significance as a hub for commerce, governance, and education (Ministry of ICT and Innovation, 2024). Its strategic

location and demographic diversity render it an ideal site for studying cybersecurity awareness within tertiary education institutions.

Nakuru County hosts a vibrant and diverse educational landscape, comprising public universities, private universities, Technical and Vocational Education and Training (TVET) institutions, and various specialized colleges. Estimates from the Ministry of ICT and Innovation (2024) indicate that there are approximately 43,500 students enrolled across tertiary institutions in the county. Specifically, public universities account for about 16,500 students, private universities host 7,000 students, TVET institutions enroll approximately 11,000 students, and specialized colleges account for 9,000 students (Ministry of ICT and Innovation, 2024). Prominent institutions in the county include Egerton University, Kabarak University, Mount Kenya University (Nakuru Campus), Kenya Medical Training College (Nakuru Campus), and Rift Valley Institute of Science and Technology (RVIST) (Gabra et al., 2022).

Documented cases of cybersecurity threats within Nakuru County's tertiary institutions reveal a worrying trend. A survey conducted among students indicated that 95.9% had experienced hacking incidents, 95.3% had encountered social media abuses, 93.8% reported exam cheating through online platforms, and 97.4% reported experiences of online extortion (Gabra et al., 2022). Although recruitment into extremist groups via digital platforms was reported by a smaller proportion (2.3%), the overall prevalence of cyber threats signifies a major security concern among the student population. Moreover, the Communications Authority of Kenya (2022) noted a substantial rise in cases of phishing attacks, social engineering scams, and financial fraud targeting students in Nakuru's tertiary institutions.

Additionally, the Kenya National Examinations Council (KNEC, 2023) reported a surge in academic dishonesty cases, facilitated through unauthorized online channels during examinations, highlighting the vulnerability of students in the digital learning environment. These developments affirm that cybersecurity threats within Nakuru County are not merely isolated incidents but represent a broader challenge confronting tertiary institution at both the individual and institutional levels.

Given Nakuru County's strategic educational importance, documented prevalence of cyber threats, and demographic diversity, the county presents a highly suitable context for examining cybersecurity threat awareness among tertiary students and exploring how awareness initiatives can contribute to the creation of secure learning environments.

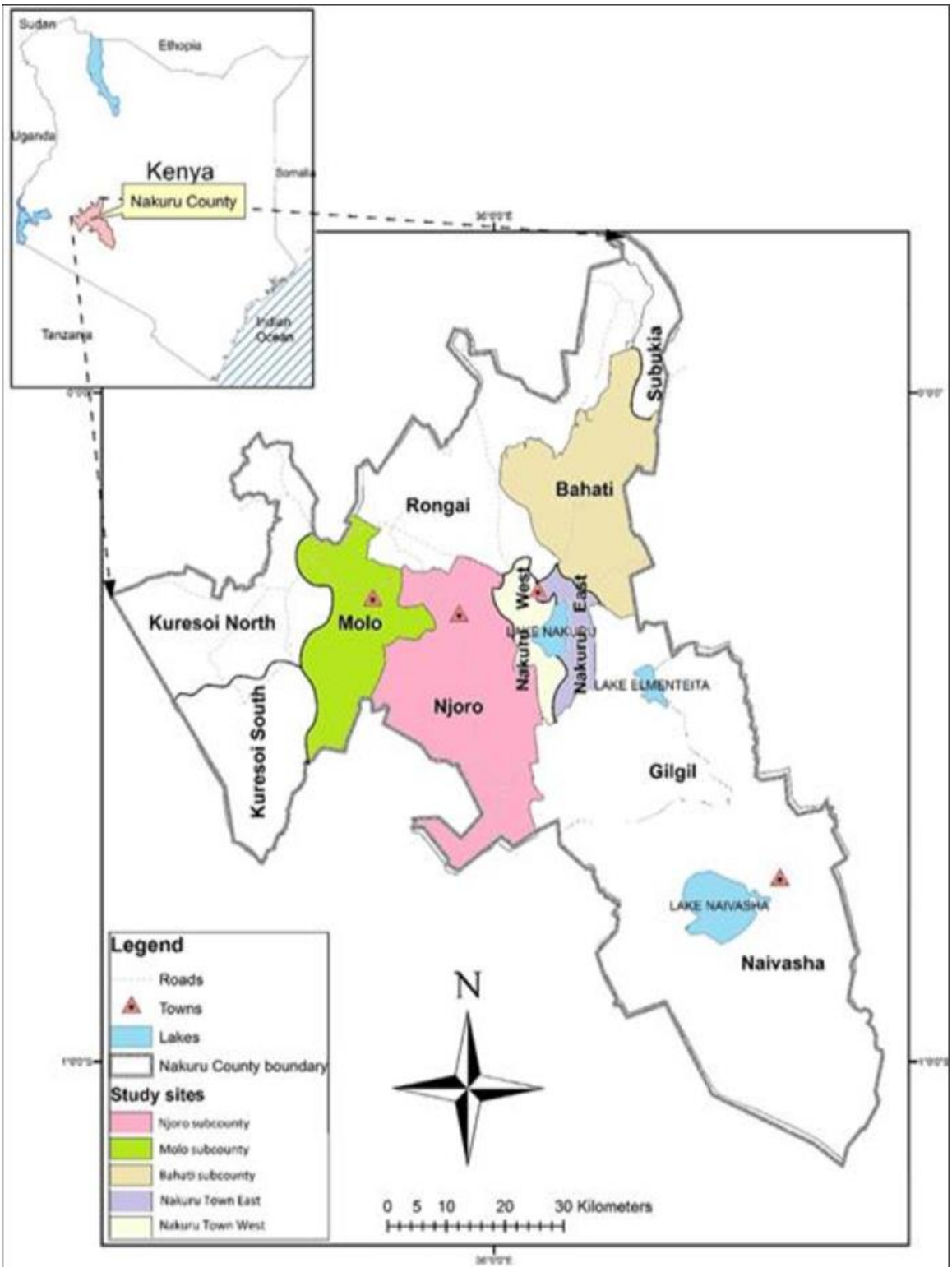


Figure 3. 1: Map of Nakuru County

3.4 Target Population

The study focused on exploring the role of cyber security threat awareness on the creation of a secure learning environment in Kenya's tertiary institutions within Nakuru County. Therefore, the ideal respondents for this study were students who were currently enrolled in tertiary institutions in Kenya. Students were directly impacted by cybersecurity policies implemented nationally and within their respective institutions, and they interacted with these policies on a regular basis, making them expected to adhere to them. As a result, they were the most suitable respondents to provide insights into their awareness and understanding of cybersecurity policies. Moreover, students' experiences with cyber security threats, such as data breaches, phishing attempts, and malware infections, provided valuable information about the prevalence and nature of cyber threats within tertiary institutions. Their firsthand accounts offered insights into the frequency and impact of such incidents. There were approximately 43,500 students in tertiary institutions in Nakuru County, Kenya (See table 3.1 and Appendix IV).

Table 3. 2: Target Population

Tertiary Institution	Estimated Number of Students	Officers
Technical and Vocational Education and Training (TVET)	11000	
Private Universities	7000	
Public Universities	16500	
Others	9000	
Administrators in TVET Institutions		20
Officer Commanding Station (OCS)		1
Total Population	43500	21

Source: Ministry of ICT and Innovation (Kenya) (2024); National Cybersecurity Strategy (2022)

Table 3.2 presents the estimated number of students in various types of tertiary institutions in Nakuru County, Kenya. The categorization of these institutions into TVET (Technical and Vocational Education and Training) colleges, private universities, public universities, and others is justified in the context of assessing the level of cyber security threat awareness among students.

Technical and Vocational Education and Training (TVET) Institutions typically offer vocational and technical training programs, focusing on practical skills development. In Nakuru County, TVET institutions cater to a significant number of students, with an estimated population of 11,000. Including TVET colleges in the study ensures representation from students pursuing technical and vocational courses, who may have specific cybersecurity awareness needs related to their field of study and future careers.

Private universities in Nakuru County, with an estimated student population of 7,000, attract students from diverse backgrounds and offer a range of academic programs. These institutions often have unique cybersecurity policies and practices compared to public universities, making it essential to include them in the study to understand the full spectrum of cyber security threat awareness among students.

Public universities, with an estimated student population of 16,500, are major educational institutions in Nakuru County. These universities offer a wide array of courses and have a significant impact on the academic landscape. Including public universities ensures representation from a large and diverse student population, allowing for a comprehensive assessment of cyber security threat awareness among tertiary students.

The category "Others" includes institutions not classified under TVET, private, or public universities. This category may encompass colleges, training institutes, or specialized institutions offering specific programs. With an estimated population of 9,000 students, these institutions contribute to the overall tertiary education sector in Nakuru County and warrant consideration in the study to capture a holistic view of cyber security threat awareness among students.

The total population of 43,500 students reflects the collective student body across different tertiary institutions in Nakuru County. By categorizing the institutions based on their type, the study can explore variations in cyber security threat awareness levels, policies, and practices among students from diverse educational backgrounds. This approach ensures a comprehensive understanding of the cyber security landscape in Nakuru County's tertiary education sector and facilitates targeted interventions to enhance students' cyber security awareness and preparedness.

3.5 Study Sample

3.5.1 Study Sample Size

The sample size was determined using the formula by Yamane, given by:

$n= N/ (1+N (e)^2)$

Where:

n = sample size

N = population size

e = margin of error (5%)

Using the formula, the sample size will be:

n =N/ (1+N(0.0025)

Therefore, the sample size of the study was 43500 respondents (National Cybersecurity Strategy, 2022), distributed as follows. The sample was distributed as shown in Table 3.2.

n =43500/ (1+43500(0.0025) = 396.3553531

Therefore, a sample size of 396 students will be utilized, and this distributed proportionately according to the population holdings in Table 3.2.

Table 3. 3: Sample Distribution Matrix

Tertiary Institution	Target Population (N)	N%	Sample Size (N% x 396)
Technical and Vocational Education and Training (TVET)	11000	25%	100
Private Universities	7000	16%	64
Public Universities	16500	38%	150
Others	9000	21%	82
Total Population	43500	100%	396

The sample size distribution for a study assessing cyber security threat awareness among students in Kenya's tertiary institutions, focusing on Nakuru County, was as follows: TVET colleges (n = 100), private universities (n = 64), public universities (n = 150), and other specialized institutions (n = 82), with a total population of 396. This distribution reflected the proportional representation of students across different types of tertiary institutions in Nakuru County. It ensured that the sample adequately captured the diversity of student populations in the county's educational landscape, allowing for comprehensive insights into cyber security threat awareness across various institutional contexts. By distributing the sample size in this manner, the study aimed to provide a holistic understanding of cyber security preparedness among students in Nakuru County's tertiary institutions, thereby facilitating the development of targeted interventions to enhance cyber security awareness and resilience within the educational sector. The sample also included 20 Information Security Officers (CISOs) and 1 Officer Commanding Station (OCS) from the target population.

3.5.2 Sampling Procedure

This study employed a combination of stratified random sampling and purposive sampling techniques to ensure both representativeness and depth of insight. Stratified random sampling was used to select students from different categories of tertiary institutions—public universities, private universities, TVET institutions, and other colleges—proportionally to their population sizes within Nakuru County. This approach ensured that each institutional type was adequately represented, capturing variations in cybersecurity awareness across different educational contexts. Stratification was based on institution type, while random selection within each stratum enhanced the generalizability and reliability of the findings by minimizing selection bias (Creswell & Creswell, 2023).

In addition to students, purposive sampling was applied to select key informants who held specialized knowledge on cybersecurity issues within their institutions. These included Information Security Officers (Chief Information Security Officers - CISOs) and the Officer Commanding Station (OCS) responsible for law enforcement related to cybercrime in Nakuru County. A total of 20 CISOs and 1 OCS were purposively selected because of their strategic positions in overseeing institutional cybersecurity policies, incident reporting mechanisms, and threat mitigation strategies. Their expert opinions were critical for providing deeper insights into institutional preparedness, existing vulnerabilities, and policy gaps. The purposive sampling ensured that individuals who possess in-depth, practical experience in cybersecurity management were included, enriching the qualitative component of the study with expert-driven perspectives (Taherdoost, 2021).

3.6 Data Collection

3.6.1 Research Instrument

The inclusion of multiple data collection tools, including questionnaires and interviews, was justified by the need for a comprehensive understanding of cyber security threat awareness among tertiary institution students in Nakuru County. Questionnaires allowed for the efficient collection of quantitative data on students' awareness levels and experiences with cyber threats, providing statistical insights into the prevalence and distribution of cyber security challenges (Creswell, 2018). Interview schedules offered an opportunity for in-depth exploration of individual perspectives and experiences, allowing researchers to gain a deeper understanding of the nuanced factors influencing cyber security awareness. Additionally, the utilization of secondary data sources such as existing literature, reports, and official documents enriched the study by providing historical context, validating primary research findings, and incorporating broader national and global perspectives on cyber security issues. Together, these data collection tools ensured a comprehensive and robust analysis of cyber security threat awareness among tertiary institution students in Nakuru County, enabling the generation of informed recommendations for policy and practice.

3.6.1.1 Questionnaires

The questionnaires were administered to undergraduate and postgraduate students enrolled in public universities, private universities, TVET institutions, and other tertiary colleges within Nakuru County. A total of 396 students were selected through stratified random

sampling to ensure proportional representation across different types of institutions. The distribution of the questionnaires was conducted both physically and electronically. For physical distribution, printed copies were delivered through institution coordinators who assisted in reaching students within lecture halls and common areas. For electronic distribution, a structured online questionnaire was sent via official student email addresses and institutional WhatsApp groups, ensuring that even students engaged in remote learning could participate. Clear instructions and consent forms accompanied both modes of distribution to enhance response rates and ensure ethical compliance during data collection.

The research questionnaire designed for this study encompassed several key sections aimed at capturing comprehensive insights into students' awareness, experiences, and knowledge pertaining to cyber security threats. Part A of the questionnaire focused on gathering demographic characteristics, allowing researchers to understand the composition of the study population and identify any potential demographic factors that may influence cyber security awareness.

In Part B, students were queried about the extent of their awareness regarding cyber security policies, including both national and institutional policies. This section aimed to assess students' familiarity with existing cyber security regulations and guidelines.

Part C focused on capturing information about the incidence of cyber security threats experienced by students. Here, students were asked to report any past encounters with cyber-attacks, data breaches, or other security incidents, providing valuable insights into the prevalence of cyber security challenges among the study population.

Part D focused on preparedness of diverse tertiary institutions in countering cybersecurity threats. It helps investigate whether institutions have provided sufficient resources for cybersecurity preparedness.

Part E investigated students' access to cyber security education, including formal coursework, workshops, or training programs dedicated to cyber security awareness and skills development. This section aimed to evaluate the availability and effectiveness of cyber security education initiatives within tertiary institutions.

Finally, Part F focused on creation of a secure learning environment. By aggregating responses from the previous sections, this section provided a holistic measure of students' knowledge, experiences, and attitudes towards cyber security threats. The questionnaire served as a structured and standardized tool for collecting quantitative data on students' cyber security threat awareness. By administering this questionnaire, researchers were able to efficiently gather comprehensive insights that enabled statistical analysis, trend identification, and correlation assessment, contributing to a deeper understanding of cyber security challenges within tertiary institutions.

3.6.1.2 Interviews

Interviews offered an opportunity for in-depth exploration of students' perspectives, experiences, and insights regarding cyber security threats. By conducting interviews with student leaders and security administrators, who were often well-informed and influential within their respective institutions, researchers were able to gain nuanced understanding and context-specific information. Student leaders provided valuable qualitative data on

institutional practices, student perceptions, and challenges related to cyber security awareness. Additionally, interviews allowed for flexibility and rapport-building, fostering open dialogue and rich data collection. The interviews also enabled researchers to gain a deeper understanding of the subtleties and complexities of cyber security threats within the tertiary institution context. By exploring the thoughts, feelings, and experiences of students and administrators, researchers were able to identify specific issues and concerns that may not have been apparent through quantitative data alone.

3.6.2 Pilot Testing of Research Instruments

To conduct pilot testing of research instruments, the researcher will select 10% of the study sample, which ensures reliability and validity without consuming excessive resources (Creswell & Creswell, 2023). The pilot study will involve administering questionnaires and conducting interviews with a subset of respondents from diverse tertiary institutions in Nakuru County. This preliminary testing will help identify ambiguities, inconsistencies, and potential challenges in the research instruments before full-scale data collection. A 10% sample is appropriate as it provides meaningful insights while maintaining statistical relevance (Taherdoost, 2021). Adjustments will be made based on pilot feedback to enhance clarity and ensure that the final instruments yield reliable and valid data (Bryman, 2022).

3.6.3 Instruments Reliability

To ensure the reliability of research instruments, the researcher will use Cronbach's Alpha, with a threshold of 0.7, as recommended for internal consistency in social science research

(Tavakol & Dennick, 2021). A pilot test will be conducted with 10% of the study sample, and responses will be analyzed to compute the Cronbach's Alpha coefficient. A value of 0.7 or higher will indicate acceptable reliability, ensuring that the questionnaire items measure the intended constructs consistently (Taber, 2020). If the reliability score is below 0.7, necessary adjustments, such as refining ambiguous questions or eliminating weak items, will be made to improve consistency before full data collection.

3.6.4 Instruments Validity

To ensure the validity of research instruments, the researcher will conduct content validity, construct validity, and face validity assessments. Content validity will be established by seeking expert opinions from scholars in military studies and defense technology to evaluate whether the research instruments comprehensively cover the study variables (Taherdoost, 2022). Construct validity will be tested through factor analysis to ensure that the items accurately measure the theoretical constructs being studied (Creswell & Creswell, 2023). Face validity will be assessed by administering the questionnaire to a small subset of respondents during the pilot study to confirm clarity and relevance. Adjustments will be made based on feedback to enhance the accuracy and credibility of the instruments.

3.6.5 Data Collection Procedure

The data collection procedures are provided in this section. The study collected both secondary and primary data. For the secondary data collection method, researchers began by compiling a comprehensive list of relevant literature, reports, and official documents related to cyber security threat awareness among tertiary institution students in Nakuru

County. They conducted thorough searches using academic databases, institutional repositories, government websites, and reputable online sources. After gathering the secondary data, researchers organized and analyzed the information, extracting key findings, trends, and insights. They critically evaluated the credibility and relevance of each source, ensuring that only reliable and up-to-date information was included in the study.

To implement the questionnaire survey, researchers designed a structured questionnaire that covered key aspects of cyber security threat awareness, including students' knowledge, perceptions, and experiences. The questionnaire was pilot-tested with a small group of students to assess its clarity, comprehensibility, and relevance. Once finalized, researchers administered the questionnaire to a stratified random sample of students from different tertiary institutions in Nakuru County. They distributed the questionnaires electronically or in print format, ensuring anonymity and confidentiality of responses. Researchers followed up with reminders and incentives to encourage participation and maximize response rates. After collecting the completed questionnaires, researchers entered the data into a statistical software program for analysis.

For the interview method, researchers identified and recruited student leaders from various tertiary institutions in Nakuru County through purposive sampling. They developed a semi-structured interview guide that covered key topics related to cyber security threat awareness, such as institutional policies, student experiences, and recommendations for improvement. Researchers conducted face-to-face or virtual interviews with the selected student leaders, allowing ample time for open-ended discussions and probing questions. They audio-recorded the interviews with participants' consent and took detailed notes to

capture relevant insights and quotations. After transcribing and analyzing the interview data, researchers identified recurring themes, patterns, and discrepancies to inform the study findings.

The study's findings were based on a comprehensive analysis of the secondary data, questionnaire survey data, and interview data. The results provided valuable insights into students' knowledge, perceptions, and experiences regarding cyber security threats in Nakuru County's tertiary institutions.

3.7 Data Analysis and Presentation

The data analysis for this study involved a combination of quantitative and qualitative techniques to comprehensively examine the research problem and derive meaningful insights. For secondary data analysis, the researchers employed a systematic approach to gather relevant information from existing sources such as academic journals, reports, and official documents related to cyber security threat awareness among tertiary institution students. The data was extracted, synthesized, and analyzed to identify key trends, patterns, and insights regarding the level of awareness, prevalent threats, and experiences of students in Nakuru County. The findings were organized thematically and presented comprehensively, using tables, charts, and graphs to visualize trends and comparisons over time.

Data extraction involved organizing and compiling all responses and observations obtained from the research instruments. This entailed transcribing interviews, compiling questionnaire responses, and summarizing key points from focus group discussions.

Following extraction, data synthesis involved organizing and categorizing the collected information into themes or categories based on commonalities and patterns. This process allowed for the identification of key trends and insights regarding students' awareness, prevalent threats, and experiences related to cyber security in Nakuru County.

The process of data synthesis involved examining the synthesized data to discern underlying relationships, associations, and implications. Statistical techniques may have been applied to quantify findings from questionnaires, while qualitative analysis methods such as thematic coding may have been employed to interpret interview and focus group data. Overall, this rigorous analytical process enabled researchers to derive meaningful conclusions and recommendations from the collected data, contributing to a deeper understanding of cyber security dynamics among students in Nakuru County.

For questionnaire data, the researchers utilized statistical software such as Statistical Package for the Social Sciences (SPSS) version 27 to analyze responses collected from the survey administered to students. Descriptive statistics such as frequencies, percentages, means, and standard deviations were calculated to summarize the data and provide an overview of students' awareness levels, perceptions, and experiences regarding cyber security threats. Inferential statistics such as correlation analysis and regression analysis may have been employed to examine relationships between variables and identify significant predictors of cyber security threat awareness among students. The results were presented using tables, charts, and graphs to facilitate interpretation and enhance the clarity of findings.

For interviews, thematic analysis was used to identify recurring themes, patterns, and insights emerging from the qualitative data collected from student leaders. Transcripts of interviews were coded and analyzed to extract relevant themes and categories related to students' perspectives, experiences, and recommendations regarding cyber security threat awareness in Nakuru County. The findings were presented in narrative form, supplemented with quotations and excerpts from interviews to illustrate key points and provide context for the analysis.

3.8 Legal and Ethical Consideration

In conducting the research on cyber security threat awareness among tertiary institution students in Nakuru County, ethical considerations were paramount throughout the entire process. Firstly, the researcher obtained a research permit from the National Commission for Science, Technology and Innovation (NACOSTI) in Kenya, ensuring compliance with regulatory requirements and ethical standards. This permit authorized the researcher to carry out the study in accordance with established guidelines and protocols. Additionally, the researcher prioritized the confidentiality and anonymity of participants by ensuring that all data collected, including responses from questionnaires, interviews, and focus group discussions, were kept confidential and used only for research purposes. Participants were assured that their identities and personal information would be protected, and data was stored securely in password-protected electronic files or locked cabinets accessible only to authorized personnel.

Informed consent was obtained from all participants before their involvement in the study, outlining the purpose, procedures, risks, and benefits of participation. Participants had the

right to withdraw from the study at any time without penalty or consequence. Moreover, the researchers adhered to principles of respect, beneficence, and justice in their interactions with participants, ensuring that their dignity, rights, and welfare were upheld throughout the research process. Any potential conflicts of interest or biases were disclosed transparently, and efforts were made to minimize their impact on the integrity and credibility of the study.

CHAPTER FOUR

DATA ANALYSIS AND FINDINGS

4.1 Introduction

This chapter is a presentation of the study's data, analysis, interpretation, and discussion. Detailed sections of data analysis in the form of descriptive analysis, descriptive statistics, and inferential statistics as guided by the methodology in Chapter Three are included in the chapter. Questionnaires, interview schedules, focus group discussions and document analysis guide were used to collect data. The analysis and presentation were guided by the objectives of the study and related to the literature review in Chapter Two.

4.2 Response Rate

Table 4.1 presents the response rate from various tertiary institutions, including Technical and Vocational Education and Training (TVET), Private Universities, Public Universities, and Others.

Table 4. 1: Response Rate

Tertiary Institution	Target - Sample Size	Actual	Response Rate
Technical and Vocational Education and Training (TVET)	100	81	81.0%
Private Universities	64	56	87.5%
Public Universities	150	128	85.3%
Others	82	76	92.7%
Total Population	396	341	86.6%

The total population targeted was 396, with 341 actual respondents, resulting in an overall response rate of 86.6%. The highest response rate was observed in the 'Others' category, with 92.7%, followed by Private Universities at 87.5% and Public Universities at 85.3%.

TVET institutions had the lowest response rate at 81.0%. According to Nutty (2008), a response rate of 75% or above is considered excellent for research studies. Therefore, the achieved response rates in this study, ranging from 81.0% to 92.7%, are well within the recommended range, indicating a strong level of engagement from participants across the diverse institutions. This high response rate enhances the reliability and validity of the findings, ensuring that the data collected accurately reflects the perspectives of the sampled population.

4.3 Presentation Analysis and Research Findings

4.3.1 Demographic Characteristics

The tables in this section provide an overview of the demographic characteristics of the respondents in a study examining the role of cybersecurity threat awareness in creating a secure learning environment in Kenya's tertiary institutions within Nakuru County. The tables cover gender distribution, age, and study level of the participants. The analysis of these demographics helps in understanding the diversity of the sample and in ensuring the representativeness of the data.

4.3.1.1 Gender Distribution

Table 4.2 shows the gender distribution of the respondents.

Table 4. 2: Gender Distribution

Response	Frequency	Percentage
Male	177	51.9
Female	164	48.1
Total	341	100

The results in Table 4.2 show that the gender distribution of the respondents shows a near-equal representation, with 177 males (51.9%) and 164 females (48.1%). This balanced distribution indicates that both genders are adequately represented in the study, which helps eliminate gender bias in understanding cybersecurity awareness and its impact on the

learning environment. This representation ensures that the findings can be generalized across both male and female populations within the tertiary institutions.

4.3.1.2 Age Distribution of Respondents

The results relating to the age distribution of respondents are provided in Table 4.3.

Table 4. 3: Age Distribution of Respondents

Response	Frequency	Percentage
18 - 25 years	237	69.5
26 – 35 years	46	13.5
36 – 45 years	58	17
Total	341	100

The age distribution results in Table 4.3 reveal that the majority of respondents, 237 (69.5%), are between 18 and 25 years old, followed by 46 respondents (13.5%) aged 26 to 35 years, and 58 respondents (17.0%) aged 36 to 45 years. This suggests that the study predominantly represents younger individuals, which aligns with the typical age range of students in tertiary institutions. The age diversity ensures that the study captures perspectives across different age groups, contributing to a comprehensive understanding of cybersecurity awareness.

4.3.1.3 Study Level of Respondents

Table 4.4 presents the distribution of respondents by study level, drawn from various educational institutions, including Technical and Vocational Education and Training (TVET) institutions, Private Universities, Public Universities, and other types of institutions.

Table 4. 4: Study Level of Respondents across Different Educational Institutions

Response	Frequency	Percentage
Certificate	145	42.5
Diploma	80	23.5

Bachelor's Degree	68	19.9
Master's Degree	48	14.1
Total	341	100

The largest group of respondents, 145 (42.5%), are at the Certificate level, followed by 80 (23.5%) at the Diploma level. Bachelor's degree students comprise 68 (19.9%) of the respondents, and Master's degree students make up 48 (14.1%). This distribution reflects a broad representation across different academic levels, which is essential for capturing a comprehensive view of cybersecurity threat awareness among students in these varied institutions. The significant representation from Certificate and Diploma students, particularly from TVET institutions, underscores the need to focus on cybersecurity awareness across all levels of education. The diverse academic backgrounds help minimize bias, ensuring the findings are applicable across different educational settings and student populations within Nakuru County.

4.3.1.4 Prevalence of Cybersecurity Threats among Students in Nakuru County's Tertiary Institutions

Table 4.5 illustrates the prevalence of various cybersecurity threats encountered by students in tertiary institutions within Nakuru County.

Table 4. 5: Prevalence of Cybersecurity Threats among Students in Nakuru County's Tertiary Institutions

		Frequency	Percentage
Femicide	Yes	233	68.3%
	No	108	31.7%
Exam cheating,	Yes	320	93.8%
	No	21	6.2%
Social media abuses	Yes	325	95.3%
	No	16	4.7%
Recruitment into extremist groups via social platforms	Yes	8	2.3%
	No	333	97.7%

Extortion	Yes	332	97.4%
	No	9	2.6%
Hacking	Yes	327	95.9%
	No	14	4.1%

The table indicates that social media abuses are the most prevalent, with 325 respondents (95.3%) having experienced them, followed closely by hacking incidents, reported by 327 respondents (95.9%). Exam cheating is also highly prevalent, with 320 students (93.8%) admitting to having encountered it. On the other hand, recruitment into extremist groups via social platforms is the least reported threat, with only 8 respondents (2.3%) acknowledging it. These results highlight the critical need for robust cybersecurity awareness programs in Nakuru County's tertiary institutions. The high prevalence of threats such as social media abuses, hacking, and extortion suggests that students are frequently exposed to significant risks, which could compromise the safety and integrity of the learning environment. Addressing these issues through targeted cybersecurity training and policies can help create a more secure educational atmosphere, reducing the likelihood of students falling victim to these threats. By identifying these prevalent threats, the study helps eliminate potential bias by focusing on the most pressing issues faced by the student population.

4.3.1.5 Experience of Cybersecurity Threats among Students – Classification of responses by Gender

Table 4.6 highlights gender differences in the experience of various cybersecurity threats among students in Nakuru County's tertiary institutions. The responses are classified by gender.

Table 4. 6: Gender Differences in the Experience of Cybersecurity Threats among Students

Cybersecurity Threats		Gender			
		Male		Female	
		F	%	F	%
Femicide	Yes	106	59.9%	127	77.4%
	No	71	40.1%	37	22.6%
Exam cheating,	Yes	168	94.9%	152	92.7%
	No	9	5.1%	12	7.3%
Social media abuses	Yes	164	92.7%	161	98.2%
	No	13	7.3%	3	1.8%
Recruitment into extremist groups via social platforms	Yes	4	2.3%	4	2.4%
	No	173	97.7%	160	97.6%
Extortion	Yes	168	94.9%	164	100.0%
	No	9	5.1%	0	0.0%
Hacking	Yes	163	92.1%	164	100.0%
	No	14	7.9%	0	0.0%

The data shows that females are more likely to have encountered femicide-related threats, with 127 (77.4%) females reporting such incidents compared to 106 (59.9%) males. Conversely, both genders reported high experiences of exam cheating, social media abuses, extortion, and hacking, with only slight variations in the percentages. For example, 164 (100.0%) females and 163 (92.1%) males reported experiencing hacking. Notably, extortion and hacking were experienced by all the female respondents (100%), with no female student indicating otherwise. These findings suggest that while certain threats, such as femicide, may disproportionately affect female students, both male and female students are significantly impacted by other cybersecurity threats. The results underscore the importance of gender-sensitive approaches in cybersecurity awareness programs, ensuring that the unique vulnerabilities faced by different genders are addressed. By examining gender differences in the experience of these threats, the study helps eliminate potential

bias by acknowledging and addressing the varied experiences of students based on their gender.

4.3.2 Extent of Awareness of Cybersecurity Policies

The following table presents descriptive statistics concerning the extent of awareness of cybersecurity policies among tertiary institution students in Nakuru County, Kenya. It captures the distribution of responses across various statements regarding awareness, understanding, training, and communication related to these policies.

4.3.2.1 Descriptive Statistics for Extent of Awareness of Cybersecurity Policies

Table 4.7 presents the descriptive statistics for the extent of awareness of cybersecurity policies among students in tertiary institutions within Nakuru County. The table summarizes the students' responses to various statements regarding students awareness and understanding of key cybersecurity policies, including data protection, network security, and acceptable use policies.

Table 4. 7: Descriptive Statistics for Extent of Awareness of Cybersecurity Policies

Statement	SD F(%)	D F(%)	N F(%)	A F(%)	SA F(%)	Mean	Std Dev.
I am aware of the data protection policy at my institution.	15 (4.4%)	14 (4.1%)	102 (29.9%)	122 (35.8%)	88 (25.8%)	3.74	1.027
I understand the key elements of the network security policy.	10 (2.9%)	15 (4.4%)	112 (32.8%)	123 (36.1%)	81 (23.8%)	3.73	0.968
I am familiar with the data acceptable use policy.	10 (2.9%)	11 (3.2%)	122 (35.8%)	118 (34.6%)	80 (23.5%)	3.72	0.955

I have received training on data protection policies.	15 (4.4%)	11 (3.2%)	106 (31.1%)	118 (34.6%)	91 (26.7%)	3.76	1.024
The institution regularly updates us on cybersecurity policies.	15 (4.4%)	12 (3.5%)	92 (27.0%)	143 (41.9%)	79 (23.2%)	3.76	0.992
I know whom to contact in case of a data breach.	7 (2.1%)	9 (2.6%)	105 (30.8%)	132 (38.7%)	88 (25.8%)	3.84	0.912

The results show that, in investigating awareness of the data protection policy at their institution, respondents indicated a fairly favorable level of knowledge, with 35.8% agreeing (A) and 25.8% strongly agreeing (SA), leading to a mean score of 3.74 and a standard deviation of 1.027. Despite this relatively positive outlook, a combined total of 8.5% (SD and D) suggests that nearly one in ten students is unaware of such critical policies. This implies a need for further engagement and training efforts, as highlighted by Wanjiru et al. (2023), who found that varying awareness levels among students directly affect their understanding of institutional commitments to cybersecurity in Kenya.

The results concerning understanding the key elements of the network security policy reveal a mean score of 3.73, with 36.1% of participants agreeing and 23.8% strongly agreeing. Although a significant proportion (32.8%) remained neutral, indicating ambivalence about their understanding, the total awareness level still presents a challenge for creating a secure learning environment. This aligns with Khan et al. (2022), who noted similar trends in Pakistan where the complexity of policy language impeded student understanding of institutional frameworks. Enhanced educational efforts and simplification of communication may therefore be critical in both contexts.

Respondents' familiarity with the data acceptable use policy revealed a mean score of 3.72, suggesting that while many students are at least somewhat aware, a concerning 6.1% expressed a lack of awareness (SD and D). This highlights a gap that could be detrimental

to cybersecurity practices within institutions, as familiarity with usage policies is vital for promoting safe online behavior. Comparable findings from Aliyu et al. (2020) indicate that many students in Nigeria possess minimal awareness of their institutions' policies despite basic knowledge of cybersecurity threats, underscoring a common challenge across various educational contexts.

The statement relating to the training received on data protection policies yielded a slightly higher mean of 3.76, with 34.6% of respondents agreeing and 26.7% strongly agreeing that they had received adequate training. Nonetheless, lower percentages of unawareness underscore the necessity for continual educational interventions. This resonates with the study by Adekunle et al. (2020), which highlighted that regular policy updates and training sessions lead to improved student engagement and compliance within Nigerian tertiary institutions.

Regarding institutional communication about cybersecurity policies, the results demonstrated a mean of 3.76, with 41.9% of respondents agreeing that their institutions regularly update them on policy changes. Despite this optimism, the 4.4% who disagreed and those neutral suggest room for improvement in communication effectiveness. This correlates with Mensah and Asante (2023), who found that perceived relevance and accessible support significantly shaped students' awareness levels, emphasizing the importance of clear institutional messaging in enhancing cybersecurity culture.

Lastly, the statement about knowing whom to contact in case of a data breach showed the highest awareness, with a mean score of 3.84, 38.7% agreeing and 25.8% strongly agreeing. This finding is encouraging as it indicates a proactive approach to awareness regarding immediate action steps in the event of an incident. Such understanding facilitates a more responsive stance to potential cyber threats. This aligns well with Mugisha's (2020) findings in Rwanda, where high awareness of cyber threats was noted but could not effectively counteract risks without substantial institutional preparedness. Further education can streamline responses to breaches, thereby enhancing the overall cybersecurity posture within educational environments.

In summary, these results indicate a moderate level of awareness regarding cybersecurity policies among tertiary institution students in Nakuru County. However, they also reveal significant gaps and areas for improvement concerning training, communication, and the practical application of these policies. Understanding and addressing these gaps will be crucial in fostering a safe and secure learning environment in Kenya's increasingly digital educational landscape.

The student leaders were asked to describe their understanding of the cybersecurity policies implemented by their institution, and the most common responses were as follows.

> Student 1 stated, "I understand that the institution has policies on data protection and acceptable use, but I'm not fully aware of the specific details." (14/10/2024)
>
> Student 5 responded, "I know there are rules about what we can and cannot do online, especially regarding protecting our personal data, but I haven't seen a detailed document explaining everything." (14/10/2024)

The student leaders were asked how aware they were of the specific cybersecurity policies and guidelines set forth by their institution, and the most common responses were as follows.

> Student 2 mentioned, "I am somewhat aware that there are guidelines, but I don't know all of them in detail." (14/10/2024)
>
> Student 4 commented, "I've heard about the cybersecurity policies during orientation, but I haven't looked into them much since then." (14/10/2024)

The student leaders were asked to share any instances where they had observed or experienced non-compliance with cybersecurity policies among students, and the most common responses were as follows.

> Student 4 stated, "I've seen students share passwords and leave their accounts logged in on public computers, which goes against the policies." (14/10/2024)

> Student 5 responded, "Some students download unauthorized software, which is a clear violation of the institution’s cybersecurity guidelines."

The responses gathered from the student leaders illustrate a concerning lack of awareness and understanding of the cybersecurity policies at their institution. While there is a general acknowledgment of the existence of guidelines regarding data protection and acceptable use, most students expressed uncertainty about the specific details and implications of these policies. This gap in knowledge is further compounded by a lack of proactive engagement with the guidelines, as many students only recall mentioning during orientation without familiarizing themselves further. Additionally, the observations of non-compliance, such as sharing passwords and downloading unauthorized software, highlight a disconnect between policy and practice. This suggests a need for enhanced education and communication around cybersecurity protocols to ensure that students not only recognize the importance of these policies but also adhere to them in practice. Overall, this situation underscores the vital need for institutions to provide clearer, more accessible information and training concerning cybersecurity, fostering a culture of awareness and compliance among students.

The security administrators were asked to describe the current cybersecurity policies and protocols in place at their institution, and the most common responses were as follows.

> Administrator 1 stated, "We have a comprehensive cybersecurity policy that covers data protection, network security, and user access controls." (14/10/2024)

> Administrator 3 responded, "Our protocols include regular updates to security software, mandatory password changes, and restricted access to sensitive information." (14/10/2024)

The security administrators were asked how the cybersecurity policies were communicated to students and faculty members, and the most common responses were as follows.

> Administrator 9 mentioned, "We use emails, the institution's website, and orientation sessions to inform students and faculty about the policies." (15/10/2024)

> Administrator 14 commented, "Policies are communicated through student handbooks, faculty meetings, and regular cybersecurity awareness campaigns." (16/10/2024)

The security administrators were asked how effective they thought these policies were in raising awareness about cybersecurity among students, and the most common responses were as follows.

> Administrator 5 stated, "The policies are effective to an extent, but continuous education and reminders are necessary to keep students aware." (14/10/2024)

> Administrator 10 responded, "While the policies are well-structured, their effectiveness is sometimes limited by students' lack of engagement." (15/10/2024)

The responses from the security administrators reflect a multifaceted approach to cybersecurity at the institution, highlighting the establishment of comprehensive policies encompassing essential areas such as data protection, network security, and user access controls. Regular security software updates and strict access measures underscore a proactive stance in maintaining a secure environment. However, despite the robust framework for communicating these policies through various channels—like emails, websites, handbooks, and awareness campaigns—there are challenges in effectively engaging the student body and faculty. Administrators expressed a need for continuous education and reminders, suggesting that while the policies are structured effectively, their actual impact is hindered by a lack of sustained engagement from users. This insight underscores the importance of not only crafting solid cybersecurity policies but also fostering an ongoing, active dialogue around them to cultivate a culture of awareness and responsibility within the institution.

4.3.2.2 Correlation between Cybersecurity Awareness and Secure Learning Environments in Tertiary Institutions

The table presents the correlation results revealing a significant relationship between the extent of awareness of cybersecurity policies and the creation of a secure learning environment in Kenya's tertiary institutions, specifically in Nakuru County.

Table 4. 8: Correlation between Cybersecurity Awareness and Secure Learning Environments in Tertiary Institutions

		Extent of Awareness of Cybersecurity Policies	Creation of a Secure Learning Environment
Extent of Awareness of Cybersecurity Policies	Pearson Correlation	1	.851**
	Sig. (2-tailed)		.000
	N	341	341
Creation of a Secure Learning Environment	Pearson Correlation	.851**	1
	Sig. (2-tailed)	.000	
	N	341	341

**. Correlation is significant at the 0.01 level (2-tailed).

The Pearson correlation coefficient is high ($r = 0.851$; $p = 0.000$), indicating a strong positive relationship between these variables. This suggests that as awareness of cybersecurity policies among students' increases, the creation of a secure learning environment also improves. In the context of Kenyan tertiary institutions, this implies that enhancing students' understanding of cybersecurity policies is crucial for fostering a safer academic environment.

4.3.3 Incidence of Cyber Security Threats Experienced by students

This section presents results related to the first objective which to investigate incidences of cyber security threats experienced by students in Nakuru County's tertiary institutions.

4.3.3.1 Descriptive Statistics Results for Incidence of Cyber Security Threats Experienced by students

The following table presents descriptive statistics on the incidence of cybersecurity threats experienced by students in Nakuru County's tertiary institutions. It captures the distribution of responses across various statements regarding exposure to cyber threats, such as fraudulent attempts to obtain sensitive information, encounters with malicious software, and concerns about the frequency of these threats. The results provide insight into students' experiences and perceptions of cybersecurity risks within their academic environments.

Table 4. 9: Descriptive Statistics Results for Incidence of Cyber Security Threats Experienced by students

Statement	SD F(%)	D F(%)	N F(%)	A F(%)	SA F(%)	Mean	Std Dev.
I have encountered fraudulent attempts to obtain sensitive information in the past.	12 (3.5%)	11 (3.2%)	93 (27.3%)	146 (42.8%)	79 (23.2%)	3.79	0.953
I have encountered malicious software designed to disrupt, damage, or gain unauthorized access to my computer systems.	10 (2.9%)	12 (3.5%)	100 (29.3%)	137 (40.2%)	82 (24.0%)	3.79	0.947
I have encountered manipulative techniques used to deceive individuals into divulging confidential information.	11 (3.2%)	9 (2.6%)	116 (34.0%)	125 (36.7%)	80 (23.5%)	3.74	0.953
I am concerned about the frequency of cyber threats.	11 (3.2%)	7 (2.1%)	109 (32.0%)	130 (38.1%)	84 (24.6%)	3.79	0.947
The institution likely employs a range of technological solutions, such as firewalls, antivirus software.	8 (2.3%)	16 (4.7%)	106 (31.1%)	119 (34.9%)	92 (27.0%)	3.79	0.970

I know how to protect myself from cyber threats.	13 (3.8%)	12 (3.5%)	113 (33.1%)	128 (37.5%)	75 (22.0%)	3.70	0.975

In examining the statement regarding encounters with fraudulent attempts to obtain sensitive information, 3.5% (F=12) of respondents strongly disagreed, and 3.2% (F=11) disagreed, while 27.3% (F=93) were neutral. A significant 42.8% (F=146) agreed, and 23.2% (F=79) strongly agreed, resulting in a mean of 3.79 and standard deviation of 0.953. These results imply that a considerable number of students have indeed encountered attempts to deceive them into divulging their sensitive data, indicating a prevalent concern regarding phishing and fraudulent activities in the digital milieu. This finding resonates with Khan et al. (2022), who highlighted the frequency of phishing incidents faced by students in higher education institutions, thereby showcasing the pervasive nature of such threats across different regions and emphasizing the need for heightened cyber security training.

Regarding the experience of malicious software, 2.9% (F=10) strongly disagreed, 3.5% (F=12) disagreed, while 29.3% (F=100) were neutral. In contrast, 40.2% (F=137) agreed, and 24.0% (F=82) strongly agreed, resulting in a mean of 3.79 and standard deviation of 0.947. This indicates a high prevalence of malware encounters among students, which can severely disrupt their academic progress. Such findings are congruent with the reports from Mensah and Asante (2023), where instances of malware were documented among students, reflecting similar vulnerabilities faced across different educational contexts in Africa.

Concerning manipulative tactics employed to deceive individuals into revealing confidential information, 3.2% (F=11) strongly disagreed, 2.6% (F=9) disagreed, 34.0% (F=116) were neutral, while 36.7% (F=125) agreed, and 23.5% (F=80) strongly agreed, resulting in a mean of 3.74 and standard deviation of 0.953. The majority of students acknowledging exposure to these manipulative techniques stress the need for reinforced efforts in cyber security education. This finding aligns with the observations made in Ntaganda (2018) regarding college students, who also experienced various deceptive practices within the cyber sphere. It accentuates the need for collaborative measures within institutions to foster awareness and resilience against such threats.

When students expressed their concerns regarding the frequency of cyber threats, 3.2% (F=11) strongly disagreed, while 2.1% (F=7) disagreed. A notable 32.0% (F=109) remained neutral, with 38.1% (F=130) agreeing, and 24.6% (F=84) strongly agreeing, resulting in a mean of 3.79 and standard deviation of 0.947. The prevalent concern among students reflects their heightened awareness of potential threats impacting their digital security. This concern is supported by insights from studies like that of Jawaid (2023), which highlighted the increased awareness of cyber risks among students during remote learning prompted by crises like the COVID-19 pandemic, reinforcing the necessity for institutions to provide ongoing support and education about these risks.

On the aspect of technological solutions provided by institutions, 2.3% (F=8) strongly disagreed, 4.7% (F=16) disagreed, while 31.1% (F=106) were neutral. Meanwhile, 34.9% (F=119) agreed, and 27.0% (F=92) strongly agreed, with a mean of 3.79 and standard deviation of 0.970. These responses indicate a general recognition of the precautions and solutions implemented by institutions, but also a potential disconnect in perceived effectiveness. This reflection aligns with findings from Li and Liu (2020), where the institutional responses to cyber security were examined, showing the importance of cultural perceptions in evaluating the effectiveness of these solutions in securing students.

Lastly, regarding self-protection against cyber threats, 3.8% (F=13) strongly disagreed, 3.5% (F=12) disagreed, while 33.1% (F=113) were neutral. A substantial 37.5% (F=128) agreed, and 22.0% (F=75) strongly agreed, yielding a mean of 3.70 and standard deviation of 0.975. The ability of students to protect themselves from cyber threats is crucial, as it suggests a level of awareness of security practices necessary for personal safety online. This self-awareness echoes the conclusions of Tan and Lim (2021), which reported similar sentiments among students, emphasizing the global necessity for educational institutions to equip students with comprehensive cyber security knowledge and practices to enhance their resilience against potential online threats.

The student leaders were asked how confident they were in recognizing common cyber threats such as phishing emails or malware attacks, and the most common responses were as follows.

> Student 7 expressed, "I feel fairly confident in recognizing phishing emails and malware, as we had some training on this." (15/10/2024)
>
> Student 8 mentioned, "I'm somewhat confident, but I think I could benefit from more specific training on identifying these threats." (15/10/2024)

The student leaders were asked about their level of knowledge regarding the potential risks associated with online activities, and the most common responses were as follows.

> Student 9 stated, "I'm aware that sharing personal information or downloading files from untrusted sources can lead to security breaches." (14/10/2024)
>
> Student 11 responded, "I know the risks exist, but I'm not always sure how to avoid them effectively." (15/10/2024)

The student leaders were asked how seriously they perceived the threat of cyber-attacks and online security breaches in their day-to-day lives, and the most common responses were as follows.

> Student 1 mentioned, "I take the threat of cyber-attacks very seriously, especially after hearing about recent incidents." (14/10/2024)
>
> Student 7 stated, "I am aware of the risks, but sometimes I think they will not affect me personally, so I don't worry too much." (15/10/2024)

The responses from the student leaders indicate a mixed level of confidence and understanding regarding cyber threats and online security risks, revealing both recognition of the dangers and a desire for more education. While students like Student 7 feel relatively secure due to prior training, others, like Student 8, suggest that their understanding is not comprehensive, highlighting a gap in knowledge that could leave them vulnerable. Additionally, while some students acknowledge the risks associated with online activities, such as Student 9, others, including Student 11, express uncertainty about how to mitigate these risks effectively. The attitude towards the severity of cyber threats also varies, with Student 1 taking the issue seriously in light of current events, whereas Student 7 appears more complacent, demonstrating a tendency to underestimate personal risk. This

juxtaposition suggests a need for enhanced training and resources to empower all students to better recognize and respond to cyber threats.

The security administrators were asked if they had observed any common cyber threats or security breaches affecting students in their institution, and the most common responses were as follows.

> Administrator 9 responded, "Phishing scams and unauthorized access attempts are among the most common threats we observe." (15/10/2024)
>
> Administrator 10 mentioned, "We frequently deal with issues like malware infections and compromised student accounts due to weak passwords." (15/10/2024)

The responses from the security administrators provide insights into the proactive strategies employed by their institution to educate students on cybersecurity best practices. Administrator 7 emphasizes the importance of accessibility and ongoing education through a structured approach that includes regular workshops and online courses, which fosters a continuous learning environment. Additionally, the integration of cybersecurity resources within the learning management system suggests a commitment to embedding this critical knowledge within the students' academic journey. On the other hand, Administrator 8 highlights a collaborative approach by engaging with external experts to conduct specialized seminars, which not only keeps the curriculum updated with the latest threats and defenses but also enriches the learning experience by providing professional insights. Together, these responses illustrate a comprehensive strategy aimed at equipping students with the necessary tools and knowledge to navigate an increasingly complex cybersecurity landscape, reflecting an institution-wide recognition of the importance of cybersecurity education in today's digital world.

4.3.3.2 Correlation between Incidence of Cyber Security Threats experienced by Students and Creation of a Secure Learning Environment

This table demonstrates the correlation between the incidence of cybersecurity threats experienced by students and the creation of a secure learning environment.

Table 4. 10: Correlation between Incidence of Cyber Security Threats experienced by Students and Creation of a Secure Learning Environment

		Incidence of Cyber Security Threats Experienced by students	Creation of a Secure Learning Environment
Incidence of Cyber Security Threats Experienced by students	Pearson Correlation	1	.863**
	Sig. (2-tailed)		.000
	N	341	341
Creation of a Secure Learning Environment	Pearson Correlation	.863**	1
	Sig. (2-tailed)	.000	
	N	341	341

**. Correlation is significant at the 0.01 level (2-tailed).

The Pearson correlation coefficient of 0.863 (p = 0.000) reflects a strong positive relationship between these variables. This indicates that higher incidences of cybersecurity threats experienced by students are associated with a more secure learning environment. In the context of Kenyan tertiary institutions, this result implies that addressing and mitigating cybersecurity threats is vital for enhancing the overall security of the academic environment. This finding is consistent with Gabra et al. (2022), who found that gaps in cybersecurity preparedness and threat management can undermine the security of academic institutions in Kenya. Additionally, it echoes the challenges reported by Mugisha (2020) in Rwanda, where the prevalence of cyber threats and limited resources impact the effectiveness of cybersecurity measures in educational settings.

4.3.4 Preparedness of Diverse Tertiary Institutions

This section presents the findings related to the third objective which sought to assess the preparedness of diverse tertiary institutions in Nakuru County to counter cyber security threats through proactive measures and effective response strategies.

4.3.4.1 Descriptive Statistics for Preparedness of Diverse Tertiary Institutions

The following table presents the results of a study examining the preparedness of diverse tertiary institutions in Nakuru County, Kenya, regarding cyber security threats awareness. The table highlights the experiences of students and staff in encountering various cyber threats, their concerns about these threats, and their knowledge of protective measures.

Table 4. 11: Preparedness of Diverse Tertiary Institutions

Statement	SD F(%)	D F(%)	N F(%)	A F(%)	SA F(%)	Mean	Std Dev.
I have encountered fraudulent attempts to obtain sensitive information in the past.	12 (3.5%)	11 (3.2%)	93 (27.3%)	146 (42.8%)	79 (23.2%)	3.74	1.013
I have encountered malicious software designed to disrupt, damage, or gain unauthorized access to my computer systems.	10 (2.9%)	12 (3.5%)	100 (29.3%)	137 (40.2%)	82 (24.0%)	3.77	0.957
I have encountered manipulative techniques used to deceive individuals into divulging confidential information.	11 (3.2%)	9 (2.6%)	116 (34.0%)	125 (36.7%)	80 (23.5%)	3.81	0.968
I am concerned about the frequency of cyber threats.	11 (3.2%)	7 (2.1%)	109 (32.0%)	130 (38.1%)	84 (24.6%)	3.78	0.996
The institution likely employs a range of technological solutions, such as firewalls, antivirus software.	8 (2.3%)	16 (4.7%)	106 (31.1%)	119 (34.9%)	92 (27.0%)	3.82	0.981

I know how to protect myself from cyber threats.	13 (3.8%)	12 (3.5%)	113 (33.1%)	128 (37.5%)	75 (22.0%)	3.83	0.929

The results show that the first statement reveals that a significant portion of respondents, 146 (42.8%), agree they have encountered fraudulent attempts to obtain sensitive information, while 93 (27.3%) remain neutral, and only a small fraction, 12 (3.5%), strongly disagree. This suggests that awareness of fraudulent activities is prevalent among tertiary institution stakeholders, indicating a need for enhanced training and resources to combat such threats effectively. The results imply a critical gap in understanding and preparedness that aligns with findings by Gabra et al. (2022), who identified similar challenges in Kenyan institutions regarding effective cyber threat responses.

In terms of exposure to malicious software, 137 (40.2%) of respondents reported having encountered such threats, suggesting a significant level of engagement with dangerous content online. Moreover, 100 (29.3%) were neutral, while only 10 (2.9%) strongly disagreed with encountering these threats. These findings reflect a concerning trend, as educational institutions should prioritize cyber hygiene programs to educate students and staff on identifying and mitigating such risks. This observation resonates with the findings of Mugisha (2020), who noted limited resources and capacity in addressing cyber threats, pointing to a broader issue affecting many institutions across Africa.

Regarding manipulative techniques designed to extract confidential information, 125 (36.7%) of participants agreed they had encountered such methods. Meanwhile, 116 (34.0%) maintain a neutral stance, indicating potential uncertainty or variability in personal experiences with these threats. Only 11 (3.2%) strongly disagreed with this statement, underscoring the deceptive nature of these threats within educational contexts. This aligns with the insights provided by Badamasi and Utulu (2021), where the varying levels of awareness and preparedness in Nigerian institutions underlined the acute need for educational initiatives addressing cyber deception.

The respondents expressed notable concerns about the frequency of cyber threats, with 130 (38.1%) affirming their worries. A smaller number, 109 (32.0%), remained neutral. This

sentiment highlights an urgent requirement for institutional support systems that address mental and emotional pressures stemming from these threats. The findings are consistent with Gabra et al. (2022), whose investigation echoed the importance of building awareness and response infrastructures in Kenyans' tertiary institutions.

Furthermore, the results indicate that 119 (34.9%) of respondents believe their institutions employ effective technological solutions like firewalls and antivirus software. However, with 106 (31.1%) remaining neutral, questions about the reliability and visibility of these security measures arise. This indicates the necessity for more transparent operational practices in cyber security within institutions. Notably, Mugisha's (2020) study in Rwanda similarly demonstrated a gap in resources and technical capacity that limited the effectiveness of implemented measures.

Finally, the statement concerning personal knowledge of self-protection from cyber threats reveals that while 128 (37.5%) feel equipped to guard against such risks, there remains a critical minority, 75 (22.0%), who do not share this confidence. This discrepancy signifies a potential vulnerability that could be exploited if systemic vulnerabilities persist. It draws attention to the importance of regular training programs to enhance self-efficacy in cyber security, echoing the calls for ongoing education as found in Badamasi and Utulu's (2021) research, which stressed the importance of institutional commitment to enhancing cyber security awareness among staff and students.

The student leaders were asked if they had personally encountered any cybersecurity threats or attacks while using digital devices or online platforms, and the most common responses were as follows.

> Student 2 responded, "Yes, I received a phishing email that looked like it was from a legitimate source, asking for my login details." (14/10/2024)
>
> Student 3 stated, "I’ve experienced malware trying to install itself after clicking on a suspicious link." (14/10/2024)

The student leaders were asked to recall any specific instances where they or someone they knew had been the victim of a cyber-attack or security breach, and the most common responses were as follows.

> Student 1 shared, "A friend of mine had their social media account hacked after responding to a phishing message." (14/10/2024)
>
> Student 5 mentioned, "I know someone who lost access to their email account after clicking on a fake password reset link." (14/10/2024)

The student leaders were asked how likely they thought students were to report cybersecurity incidents or breaches to the relevant authorities, and the most common responses were as follows.

> Student 6 commented, "I think students are hesitant to report incidents because they might not know where to go or they're embarrassed." (15/10/2024)
>
> Student 7 stated, "Some students would report incidents, especially if they are serious, but others might just ignore them." (15/10/2024)

The responses from the student leaders vividly illustrate a troubling landscape of cybersecurity awareness and victimization among their peers. Several students recounted personal encounters with cyber threats, such as phishing emails and malware, indicating a prevalent vulnerability in their online behaviors. These experiences culminate in real-life consequences, as exemplified by accounts of friends falling victim to social media hacks and fraudulent activities, suggesting a wider trend of cyber insecurity within their community. The hesitance to report these incidents stems from a mix of confusion about reporting channels and a fear of being judged or embarrassed, which further exacerbates the issue by allowing potential threats to persist and proliferate unchecked. The overall narrative underscores a critical need for enhanced cybersecurity education and support systems to empower students to recognize, address, and report such incidents effectively.

The student leaders were asked if they were aware of any of their peers who had been targeted or victimized by cybersecurity threats, and the most common responses were as follows.

> Student 8 mentioned, "Yes, I know a few people who have been scammed online or had their accounts hacked." (15/10/2024)
>
> Student 9 responded, "I have heard stories from classmates about losing money through online fraud." (15/10/2024)

The student leaders were asked if they or their peers had ever discussed incidents involving cybersecurity breaches or attacks within their academic or social circles, and the most common responses were as follows.

> Student 5 stated, "We sometimes talk about these incidents, especially when they happen to someone we know." (14/10/2024)
>
> Student 11 commented, "Yes, it's a topic that comes up occasionally, usually when someone has just experienced an issue." (16/10/2024)

The student leaders were asked how effective they thought students were in identifying and reporting instances of cybersecurity threats affecting their peers, and the most common responses were as follows.

> Student 3 stated, "I think some students are good at recognizing threats, but reporting them is still an issue." (14/10/2024)
>
> Student 10 responded, "There's awareness, but I'm not sure if everyone knows how to report these incidents properly." (15/10/2024)

The feedback from the student leaders reveals a significant awareness of cybersecurity threats within their community, as many students can identify peers who have experienced online scams or account hacks. This recognition highlights the growing prevalence of such threats in their daily lives, fostering discussions about these issues, albeit in a reactive manner typically prompted by personal experiences within their social circles. While there

is an understanding of the importance of identifying cybersecurity threats, a concerning gap exists in students' knowledge and ability to report these incidents effectively. This suggests a need for enhanced educational initiatives aimed at equipping students not only with the skills to recognize potential cybersecurity threats but also with the knowledge of proper reporting protocols to ensure a safer online environment for their peers.

The security administrators were asked about the measures their institution takes to ensure students are adequately trained on cybersecurity best practices, and the most common responses were as follows.

> Administrator 7 mentioned, "We offer regular workshops, online courses, and provide access to cybersecurity resources through our learning management system." (15/10/2024)
>
> Administrator 8 stated, "Our institution collaborates with external experts to conduct seminars and training sessions on the latest cybersecurity threats and defenses." (15/10/2024)

The feedback from the security administrators highlights a proactive approach to equipping students with essential cybersecurity knowledge and skills. Administrator 7's emphasis on regular workshops and online courses suggests a commitment to continuous learning, ensuring that students not only receive foundational training but also have the opportunity to engage with up-to-date content through accessible platforms like a learning management system. Meanwhile, Administrator 8's mention of collaboration with external experts indicates a recognition of the need for specialized insights and training on the evolving landscape of cybersecurity threats, thereby enhancing the institution's overall security posture. Together, these approaches reflect a multi-faceted strategy that emphasizes both accessibility and expertise, reinforcing the importance of student awareness and preparedness in an increasingly digital and risk-prone educational environment.

The security administrators were asked how their institution monitors and detects potential cybersecurity incidents, and the most common responses were as follows.

> Administrator 9 stated, "We use real-time monitoring tools, intrusion detection systems, and regular audits to keep track of potential threats." (15/10/2024)
>
> Administrator 13 responded, "Our IT department runs continuous network scans and uses analytics to detect anomalies that could indicate a security breach." (16/10/2024)

The security administrators were asked what steps were taken to respond to and mitigate cybersecurity incidents once they were detected, and the most common responses were as follows.

> Administrator 2 commented, "We have an incident response team that acts quickly to isolate affected systems and mitigate the impact." (14/10/2024)
>
> Administrator 13 mentioned, "Our protocol includes immediate notification to stakeholders, system restoration, and a thorough investigation to prevent recurrence." (16/10/2024)

The responses from the security administrators illustrate a multi-faceted approach to cybersecurity, emphasizing both proactive monitoring and reactive incident response. Real-time monitoring tools and intrusion detection systems, as mentioned by Administrator 9, are essential for early identification of potential threats, supported by regular audits to ensure compliance and identify vulnerabilities. Administrator 13 further highlights the importance of continuous network scanning and anomaly detection through analytics, demonstrating an ongoing commitment to vigilance against breaches. In terms of response, the establishment of an incident response team, as referenced by Administrator 2, signifies a structured and swift approach to containment and damage control, while the procedures outlined by Administrator 13 such as stakeholder notifications, system restoration, and thorough investigations underscore a commitment to both immediate recovery and long-term security improvements. Together, these responses indicate that the institution prioritizes a comprehensive strategy that encompasses both preventive and remedial measures in the face of evolving cybersecurity threats.

4.3.4.2 Correlation between Preparedness of Diverse Tertiary Institutions and Creation of a Secure Learning Environment

This table illustrates the correlation between the preparedness of diverse tertiary institutions and the creation of a secure learning environment.

Table 4. 12: Correlation between Preparedness of Diverse Tertiary Institutions and Creation of a Secure Learning Environment

		Preparedness of Diverse Tertiary Institutions	Creation of a Secure Learning Environment
Preparedness of Diverse Tertiary Institutions	Pearson Correlation	1	.848**
	Sig. (2-tailed)		.000
	N	341	341
Creation of a Secure Learning Environment	Pearson Correlation	.848**	1
	Sig. (2-tailed)	.000	
	N	341	341

**. Correlation is significant at the 0.01 level (2-tailed).

The Pearson correlation coefficient of 0.848 ($p = 0.000$) signifies a strong positive relationship, indicating that higher levels of institutional preparedness are associated with more secure learning environments. In the context of Kenyan tertiary institutions, this suggests that improving institutional readiness—through measures such as enhanced cybersecurity infrastructure, staff training, and threat management—contributes significantly to the overall security of the learning environment. This finding is supported by Gabra et al. (2022), who emphasized the importance of robust cybersecurity measures and preparedness in Kenyan institutions. Additionally, it aligns with Badamasi and Utulu's

(2021) study in Nigeria, which highlighted the disparities in institutional preparedness and the need for increased investment and collaboration to enhance cybersecurity readiness.

The security administrators were asked what additional measures or resources they believed could improve cybersecurity awareness and preparedness among students in tertiary institutions, and the most common responses were as follows.

> Administrator 8 responded, "More frequent and mandatory training sessions, coupled with continuous assessments, could greatly enhance awareness."
>
> Administrator 11 mentioned, "Investing in advanced cybersecurity tools and creating a more interactive learning environment for students would be beneficial."

The responses from the security administrators highlight a dual approach to improving cybersecurity awareness among tertiary institution students. Administrator 8 emphasizes the importance of regular, mandatory training and ongoing assessments, suggesting that consistent engagement with the material will lead to better retention and understanding of cybersecurity principles. This implies that awareness should not be a one-off initiative, but rather an integral part of the educational curriculum. On the other hand, Administrator 11 advocates for the incorporation of advanced cybersecurity tools and an interactive learning environment, pointing towards the necessity of practical, hands-on experiences that can make learning more engaging and applicable to real-world scenarios. Together, these perspectives suggest that a combination of structured training and innovative learning methods may significantly foster a more robust cybersecurity culture among students, thus better preparing them to navigate the increasingly complex digital landscape.

4.3.5 Access to Cybersecurity Education

This section presents the results related to access to cybersecurity education among respondents. It includes data on the availability of cybersecurity courses, the level of participation in such courses, and the adequacy of resources provided for cybersecurity education. The findings offer insights into how well-equipped institutions are in providing the necessary education to create a secure learning environment.

4.3.5.1 Perception of Cybersecurity Education and Resources in Tertiary Institutions

Table 4.13 presents the findings of a study assessing access to cybersecurity education and resources in tertiary institutions within Nakuru County, Kenya. The table illustrates student perceptions and experiences concerning the integration of cybersecurity within the academic curriculum and the availability of resources aimed at fostering a secure learning environment.

Table 4. 103: Perception of Cybersecurity Education and Resources in Tertiary Institutions

Statement	SD F(%)	D F(%)	N F(%)	A F(%)	SA F(%)	Mean	Std Dev.
Cybersecurity is integrated into my curriculum.	24 (7.0%)	57 (16.7%)	75 (22.0%)	86 (25.2%)	99 (29.0%)	3.525	1.261
There are adequate resources available for learning about cybersecurity.	19 (5.6%)	50 (14.7%)	90 (26.4%)	79 (23.2%)	103 (30.2%)	3.578	1.217
I receive regular training on cybersecurity.	29 (8.5%)	65 (19.1%)	72 (21.1%)	73 (21.4%)	102 (29.9%)	3.452	1.320
I have access to up-to-date cybersecurity tools for learning.	21 (6.2%)	73 (21.4%)	71 (20.8%)	74 (21.7%)	102 (29.9%)	3.478	1.285
My institution encourages participation in cybersecurity workshops.	25 (7.3%)	54 (15.8%)	84 (24.6%)	92 (27.0%)	86 (25.2%)	3.469	1.231

Cybersecurity education is a priority at my institution.	23 (6.7%)	55 (16.1%)	86 (25.2%)	89 (26.1%)	88 (25.8%)	3.481	1.224

The results in Table 4.13 show that the first statement examined whether cybersecurity is integrated into the curriculum. The results indicate that 7.0% strongly disagreed (Strongly Disagree F(7.0%)), 16.7% disagreed (Disagree F(16.7%)), 22.0% remained neutral (Neither Agree nor Disagree F(22.0%)), 25.2% agreed (Agree F(25.2%)), and 29.0% strongly agreed (Strongly Agree F(29.0%)). With a mean score of 3.525 and a standard deviation of 1.261, these results imply that a significant number of students believe that there is a positive integration of cybersecurity into their curricula. This finding supports Wanjiru et al. (2023), which highlights the necessity of active curricular engagement in fostering awareness of cybersecurity policies among students in Kenyan tertiary institutions.

The second statement focused on the adequacy of resources available for learning about cybersecurity. Responses showed 5.6% strongly disagreed (Strongly Disagree F(5.6%)), 14.7% disagreed (Disagree F(14.7%)), 26.4% were neutral (Neither Agree nor Disagree F(26.4%)), 23.2% agreed (Agree F(23.2%)), and 30.2% strongly agreed (Strongly Agree F(30.2%)). The mean rating of 3.578 and a standard deviation of 1.217 suggest that most students feel that there are sufficient resources for learning about cybersecurity. This aligns with findings from Khan et al. (2022), which revealed that having adequate resources significantly contributes to increasing students' awareness of cybersecurity policies in educational contexts.

Responses regarding regular training on cybersecurity revealed that 8.5% strongly disagreed (Strongly Disagree F(8.5%)), 19.1% disagreed (Disagree F(19.1%)), 21.1% were neutral (Neither Agree nor Disagree F(21.1%)), 21.4% agreed (Agree F(21.4%)), and 29.9% strongly agreed (Strongly Agree F(29.9%)). With a mean of 3.452 and a standard deviation of 1.320, these results suggest that while a substantial number of students receive

training on cybersecurity, there remains a noteworthy portion that does not. This supports findings from Mensah and Asante (2023), where students expressed a need for enhanced training programs related to cybersecurity education for better alignment with institutional policies.

The next statement assessed access to up-to-date cybersecurity tools for learning. Findings indicated that 6.2% strongly disagreed (Strongly Disagree F(6.2%)), 21.4% disagreed (Disagree F(21.4%)), 20.8% were neutral (Neither Agree nor Disagree F(20.8%)), 21.7% agreed (Agree F(21.7%)), and 29.9% strongly agreed (Strongly Agree F(29.9%)). The mean score of 3.478 and a standard deviation of 1.285 reflect a general perception that while there is access to cybersecurity tools, not all students fully experience this access. Previous research in Uganda by Mugisha (2020) supports this perspective, highlighting similar challenges in accessing up-to-date cybersecurity resources among tertiary institutions.

On the question of institutional encouragement for participation in cybersecurity workshops, the results showed that 7.3% strongly disagreed (Strongly Disagree F(7.3%)), 15.8% disagreed (Disagree F(15.8%)), 24.6% remained neutral (Neither Agree nor Disagree F(24.6%)), 27.0% agreed (Agree F(27.0%)), and 25.2% strongly agreed (Strongly Agree F(25.2%)). With a mean of 3.469 and a standard deviation of 1.231, the responses indicate a moderate encouragement of such workshops, suggesting that further institutional effort is needed. This resonates with findings from Ariffin and Lim (2021), highlighting the importance of proactive initiatives to enhance cybersecurity engagement among students.

Lastly, the perception of cybersecurity education as a priority within institutions was assessed. Results found that 6.7% strongly disagreed (Strongly Disagree F(6.7%)), 16.1% disagreed (Disagree F(16.1%)), 25.2% were neutral (Neither Agree nor Disagree F(25.2%)), 26.1% agreed (Agree F(26.1%)), and 25.8% strongly agreed (Strongly Agree F(25.8%)). The mean of 3.481 with a standard deviation of 1.224 suggests that a significant portion of students believes cybersecurity education is prioritized but indicates room for improvement. This links back to findings by Aliyu et al. (2021), demonstrating that

prioritization not only fosters awareness but also compliance with cybersecurity policies in educational environments.

4.3.5.2 Correlation between Access to Cybersecurity Education and Creation of a Secure Learning Environment

This table presents the correlation between access to cybersecurity education and the creation of a secure learning environment.

Table 4. 14: Correlation between Access to Cybersecurity Education and Creation of a Secure Learning Environment

		Access to Cybersecurity Education	Creation of a Secure Learning Environment
Access to Cybersecurity Education	Pearson Correlation	1	.816**
	Sig. (2-tailed)		.000
	N	341	341
Creation of a Secure Learning Environment	Pearson Correlation	.816**	1
	Sig. (2-tailed)	.000	
	N	341	341

**. Correlation is significant at the 0.01 level (2-tailed).

The Pearson correlation coefficient of 0.816 ($p = 0.000$) indicates a strong positive relationship, suggesting that increased access to cybersecurity education is significantly associated with the development of a secure learning environment. In the context of Kenyan tertiary institutions, this implies that providing students with comprehensive cybersecurity education can play a crucial role in enhancing the security of their academic environment. This finding aligns with Ariffin and Lim (2021) in Malaysia, who found that integrating cybersecurity education into academic programs fosters greater awareness and compliance, leading to a more secure learning environment. Additionally, the results are consistent with Wanjiru et al. (2023) in Kenya, which highlighted that access to cybersecurity training and resources significantly influences students' engagement in cybersecurity practices.

4.3.6 Creation of a Secure Learning Environment

This section presents the results related to cybersecurity awareness and confidence in tertiary institutions. Table 4.10 illustrates the perceptions of cybersecurity awareness among students in Kenya's tertiary institutions, specifically highlighting their ability to identify risks, understand preventive measures, and recognize warning signs, among other factors. The results presented will provide valuable insights into the overall awareness levels concerning cybersecurity threats and the role of awareness in creating a secure learning environment.

Table 4. 15: Perception of Cybersecurity Awareness and Confidence in Tertiary Institutions

Statement	SD F(%)	D F(%)	N F(%)	A F(%)	SA F(%)	Mean	Std Dev.
I can identify cybersecurity risks in my learning environment.	6 (1.8%)	19 (5.6%)	104 (30.5%)	116 (34.0%)	96 (28.2%)	3.812	0.967
I understand the preventive measures to avoid cybersecurity threats.	7 (2.1%)	21 (6.2%)	107 (31.4%)	121 (35.5%)	85 (24.9%)	3.751	0.967
I recognize warning signs of potential cyber threats.	12 (3.5%)	16 (4.7%)	105 (30.8%)	130 (38.1%)	78 (22.9%)	3.721	0.983
My institution provides a secure online environment for learning.	11 (3.2%)	16 (4.7%)	110 (32.3%)	122 (35.8%)	82 (24.0%)	3.727	0.985
I feel confident using online resources without compromising security.	9 (2.6%)	20 (5.9%)	109 (32.0%)	114 (33.4%)	89 (26.1%)	3.745	0.995
My peers are also aware of the	9 (2.6%)	21 (6.2%)	117 (34.3%)	113 (33.1%)	81 (23.8%)	3.692	0.986

importance of cybersecurity.

The first statement reveals that 6 (1.8%) students strongly disagreed and 19 (5.6%) disagreed with the notion that they could identify cybersecurity risks in their learning environment. Conversely, a more considerable portion—104 (30.5%) was neutral, while 116 (34.0%) agreed, and 96 (28.2%) strongly agreed. This distribution indicates a significant level of confidence among students regarding their ability to recognize cybersecurity risks but also points to a noteworthy proportion of neutrality. This suggests a gap in effective cybersecurity education and engagement. Wanjiru et al. (2023) also noted similar findings in their study, indicating that the visibility of cybersecurity measures significantly influences students' confidence in identifying potential threats, thus underlining a need for proactive educational initiatives in cybersecurity within Kenyan institutions.

Regarding preventive measures, 7 (2.1%) of the respondents strongly disagreed, and 21 (6.2%) disagreed with the statement that they understood the preventive measures to avoid cybersecurity threats. While 107 (31.4%) were neutral, 121 (35.5%) agreed and 85 (24.9%) strongly agreed. The majority of students have a positive perception of their understanding of preventive measures, but the neutral responses indicate that many students may not actively engage or feel adequately informed on this topic. Similarly, Khan et al. (2022) found that students in Pakistan recognized the importance of understanding cybersecurity policies but often lacked detailed knowledge of these policies, suggesting that similar educational efforts could enhance knowledge in both Kenya and Pakistan.

When it comes to recognizing warning signs of potential cyber threats, the results indicated that 12 (3.5%) strongly disagreed and 16 (4.7%) disagreed with this statement. A total of 105 (30.8%) remained neutral, while 130 (38.1%) agreed and 78 (22.9%) strongly agreed. Despite a relatively high level of agreement, the substantial neutrality suggests that a substantial number of students might require more dedicated instruction on recognizing warning signs. In Ghana, Mensah and Asante (2023) highlighted that awareness levels can vary significantly in understanding cybersecurity policies, emphasizing the importance of targeted educational programs to bridge these gaps in awareness.

In evaluating whether institutions provide a secure online environment, the responses were similarly mixed, with 11 (3.2%) strongly disagreeing and 16 (4.7%) disagreeing. Meanwhile, 110 (32.3%) were neutral, 122 (35.8%) agreed, and 82 (24.0%) strongly agreed. While a significant majority view their institutions as providing a secure online learning environment, the neutral responses reflect skepticism about the institutions' actual capabilities in providing such a secure environment. This resonates with Gabra et al. (2022), who reported gaps in the overall preparedness of institutions in Kenya, necessitating firm commitments and structured approaches to enhance cybersecurity infrastructure.

On confidence in using online resources without compromising security, the results showed that 9 (2.6%) strongly disagreed and 20 (5.9%) disagreed. A significant portion, 109 (32.0%) remained neutral, while 114 (33.4%) agreed, and 89 (26.1%) strongly agreed. The results denote that many students feel relatively confident but underline the need for comprehensive cybersecurity education. This lack of full confidence mirrors findings from the literature, where Wanjiru et al. (2023) indicated that students' overall awareness correlates significantly with their confidence levels when engaging with digital resources in their institutions.

Lastly, when assessing peers' awareness of the importance of cybersecurity, 9 (2.6%) strongly disagreed, and 21 (6.2%) disagreed, whereas the neutral responses comprised 117 (34.3%), 113 (33.1%) agreed, and 81 (23.8%) strongly agreed. This indicates a moderate belief in peer awareness but suggests that collective awareness could be insufficient. This aligns with observations by Aliyu et al. (2020), who found that many students demonstrated only basic knowledge of cybersecurity threats but lacked awareness of protective measures, indicating a necessity for educational interventions targeting peer-to-peer discussions on cybersecurity in Kenyan tertiary institutions. Overall, the findings emphasize a critical need for targeted educational initiatives, proactive engagement from institutions, and enhanced policy enforcement, all aimed at fostering a culture of cybersecurity awareness among students.

The student leaders were asked how integrated they felt cybersecurity education was within their academic curriculum, and the most common responses were as follows.

> Student 3 mentioned, "Cybersecurity is touched on in some courses, but it is not deeply integrated into the curriculum." (14/10/2024)
>
> Student 7 stated, "I do not think cybersecurity education is well-integrated; it's more of an afterthought in most programs." (15/10/2024)

The student leaders were asked what resources they believed were available to students to enhance their understanding of cybersecurity concepts and practices, and the most common responses were as follows.

> Student 5 commented, "We have access to some online courses and workshops, but they are not mandatory." (14/10/2024)
>
> Student 9 responded, "There are a few resources, like seminars and guest lectures, but they are not widely advertised." (15/10/2024)

The student leaders were asked how frequently students were provided with training or workshops on cybersecurity awareness and best practices, and the most common responses were as follows.

> Student 7 mentioned, "Training sessions are offered, but they are infrequent—maybe once or twice a year." (15/10/2024)
>
> Student 8 stated, "Workshops are available occasionally, but I think they should be held more regularly." (15/10/2024)

The feedback from student leaders regarding cybersecurity education within their academic curriculum reveals a significant gap in integration and accessibility of resources. Students noted that while cybersecurity is occasionally referenced in certain courses, it lacks comprehensive incorporation in their overall academic experience, often appearing as an afterthought rather than a foundational element. This perception is echoed in their assessment of available resources for enhancing cybersecurity understanding, which are

viewed as limited and not mandatory—highlighting a missed opportunity for foundational learning. Furthermore, the infrequency of training sessions and workshops indicates that students are not sufficiently engaged with crucial cybersecurity concepts and practices. Overall, the responses suggest a pressing need for academic institutions to enhance the integration of cybersecurity into their curricula, make resources more accessible, and provide more regular training opportunities to prepare students effectively for the complexities of the digital landscape.

4.4 Regression Analysis

The section on regression analysis delves into understanding the factors influencing the creation of a secure learning environment within tertiary institutions in Nakuru County, Kenya. The analysis focuses on key predictors: Access to Cybersecurity Education, Extent of Awareness of Cybersecurity Policies, Preparedness of Diverse Tertiary Institutions, and the Incidence of Cyber Security Threats Experienced by students. By exploring the relationship between these variables and the dependent variable, which is the creation of a secure learning environment.

4.4.1 Model Summary

Table 4.16 presents the results of a regression analysis examining the influence of Access to Cybersecurity Education, Extent of Awareness of Cybersecurity Policies, Preparedness of Diverse Tertiary Institutions, and the Incidence of Cyber Security Threats Experienced by students on the Creation of a Secure Learning Environment.

Table 4.16: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.899[a]	.808	.806	.33676

a. Predictors: (Constant), Access to Cybersecurity Education, Extent of Awareness of Cybersecurity Policies, Preparedness of Diverse Tertiary Institutions, Incidence of Cyber Security Threats Experienced by students

The model shows a strong positive relationship, with an R value of .899, indicating that the predictors collectively explain 80.8% of the variance in creating a secure learning environment ($R^2 = .808$). The adjusted R^2 value of .806 suggests that the model is highly reliable, and the standard error of the estimate (.33676) indicates a good fit. The ANOVA results further support the model's significance ($F(4, 336) = 354.555$, $p < .001$), showing that the independent variables significantly contribute to the dependent variable, highlighting the critical role of cybersecurity education and related factors in fostering a secure learning environment.

4.4.2 ANOVA Results for Regression Model on Creation of a Secure Learning Environment

Table 4.17 presents the ANOVA results for the regression model predicting the creation of a secure learning environment.

Table 4.17: ANOVA Results for Regression Model on Creation of a Secure Learning Environment

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	160.840	4	40.210	354.555	.000[b]
	Residual	38.106	336	.113		
	Total	198.946	340			

a. Dependent Variable: Creation of a Secure Learning Environment
b. Predictors: (Constant), Access to Cybersecurity Education, Extent of Awareness of Cybersecurity Policies, Preparedness of Diverse Tertiary Institutions, Incidence of Cyber Security Threats Experienced by students

The analysis reveals that the model is statistically significant, with an F-value of 354.555 and a p-value less than .001, indicating that the predictors: Access to Cybersecurity Education, Extent of Awareness of Cybersecurity Policies, Preparedness of Diverse Tertiary Institutions, and Incidence of Cyber Security Threats Experienced by students collectively contribute to the model. The regression sum of squares (160.840) is substantially higher than the residual sum of squares (38.106), suggesting that a large portion of the variance in the creation of a secure learning environment is explained by the

model, underscoring the importance of these factors in shaping cybersecurity outcomes in tertiary institutions.

4.4.3 Coefficients for Predictors of Creating a Secure Learning Environment

Table 4.18 presents the coefficients for the regression analysis conducted to determine the impact of various factors on the creation of a secure learning environment. This analysis focuses on four predictors: Extent of Awareness of Cybersecurity Policies, Incidence of Cyber Security Threats Experienced by students, Preparedness of Diverse Tertiary Institutions, and Access to Cybersecurity Education. The table provides insights into the relative strength and significance of each predictor in contributing to the creation of a secure learning environment.

Table 4. 18: Coefficients for Predictors of Creating a Secure Learning Environment

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.121	.099		1.228	.220
	Extent of Awareness of Cybersecurity Policies	.257	.057	.249	4.528	.000
	Incidence of Cyber Security Threats Experienced by students	.310	.060	.303	5.165	.000
	Preparedness of Diverse Tertiary Institutions	.228	.057	.223	4.033	.000
	Access to Cybersecurity Education	.176	.046	.179	3.801	.000

a. Dependent Variable: Creation of a Secure Learning Environment

Table 4.18 presents the coefficients for the predictors of creating a secure learning environment. The constant value (.121, $p = .220$) is not statistically significant, indicating that without the influence of the predictors, the baseline level of creating a secure learning environment is minimal. The Extent of Awareness of Cybersecurity Policies shows a significant positive effect ($\beta = .257$, $p < .001$), suggesting that increased awareness is a crucial factor in enhancing security. Similarly, the Incidence of Cyber Security Threats Experienced by students has a strong positive influence ($\beta = .310$, $p < .001$), indicating that students' experiences with threats drive the need for a secure environment. Preparedness of Diverse Tertiary Institutions ($\beta = .228$, $p < .001$) and Access to Cybersecurity Education ($\beta = .176$, $p < .001$) are also significant, reinforcing that well-prepared institutions and adequate access to education are vital for creating a secure learning environment.

4.4.2 Residuals Statistics for Predictors of Creation of a Secure Learning Environment

The table 4.19 presents the residuals statistics for the regression model predicting the creation of a secure learning environment.

Table 4.19: Residuals Statistics for Predictors of Creation of a Secure Learning Environment

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	1.7791	4.7331	3.7742	.68779	341
Residual	-1.10340	1.07974	.00000	.33478	341
Std. Predicted Value	-2.901	1.394	.000	1.000	341
Std. Residual	-3.276	3.206	.000	.994	341

a. Dependent Variable: Creation of a Secure Learning Environment

The predicted values range from 1.7791 to 4.7331, with a mean of 3.7742 and a standard deviation of 0.68779, indicating variability in the predicted scores. The residuals, representing the difference between observed and predicted values, range from -1.10340 to 1.07974, with a mean of 0.00000 and a standard deviation of 0.33478. This suggests that the model's predictions are reasonably accurate, with most residuals close to zero, indicating that the model explains a substantial portion of the variance in the creation of a secure learning environment. The standardized predicted values and residuals further confirm the model's accuracy, as the standard deviations are close to 1, and the means are near 0. These results imply that the model effectively captures the relationship between the predictors and the dependent variable in the context of cybersecurity in Kenyan tertiary institutions. This is supported by the normal distribution in Figure 2.

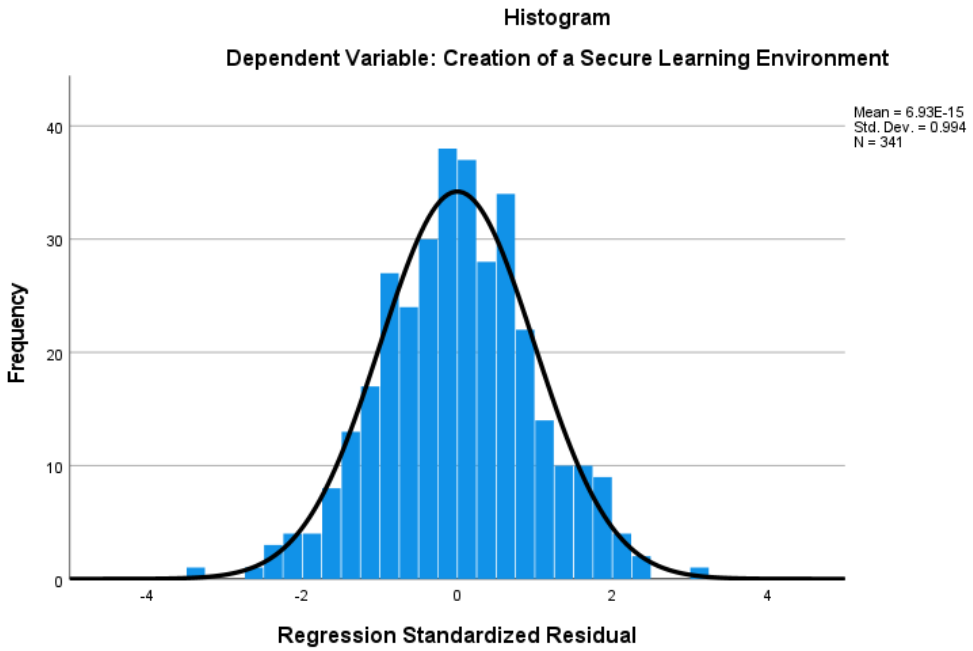


Figure 4. 1: Regression Histogram

CHAPTER FIVE

DISCUSSIONS, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter presents the summary, conclusions, and recommendations of the study. The purpose of this study is to explore the role of cyber security threat awareness on creation of a secure learning environment in Kenya's tertiary institutions within Nakuru County. The chapter contains a summary of the study findings, the conclusion, recommendations, and suggestions for further studies.

The objectives that guided the study were:

i) To determine the extent to which students in Nakuru County's tertiary institutions are aware of cyber security policies.
ii) To investigate incidences of cyber security threats experienced by students in Nakuru County's tertiary institutions.
iii) To assess the preparedness of diverse tertiary institutions in Nakuru County to counter cyber security threats through proactive measures and effective response strategies.

5.2 Discussions

5.2.1 Extent of Awareness of Cybersecurity Policies

The study findings indicate a moderate level of awareness of cybersecurity policies among students in tertiary institutions in Nakuru County, with a notable proportion displaying familiarity with key cybersecurity policies such as data protection and acceptable use policies. This aligns with the Protection Motivation Theory (PMT), which posits that individuals are more likely to adopt protective behaviors when they perceive threats and understand effective coping mechanisms (Rogers, 1975). The moderate awareness

suggests that while some students recognize cybersecurity risks, gaps in training and communication hinder the full adoption of secure behaviors.

This result is consistent with prior literature that emphasizes the role of institutional policies in fostering cybersecurity awareness among students (Mensah & Asante, 2023). However, the findings also revealed that a significant number of students remained unaware of whom to contact in the event of a cybersecurity incident, a gap that raises concerns about the effectiveness of institutional communication strategies. In this study, interviews were conducted with purposively selected student leaders and institutional security administrators to supplement the quantitative findings and provide deeper insights into cybersecurity awareness and institutional preparedness. Student leaders, including student union representatives, club leaders, and peer mentors from various tertiary institutions, were chosen because of their influential roles and their ability to articulate the collective cybersecurity experiences, challenges, and perceptions of the wider student body. Information Security Officers (CISOs) and the Officer Commanding Station (OCS) handling cybercrime in Nakuru County were also interviewed due to their direct involvement in developing, implementing, and monitoring cybersecurity strategies within their respective institutions. This approach was justified as interviews allowed the study to capture rich, context-specific experiences that could not be fully obtained through questionnaires alone. For example, as revealed in Chapter Four, security administrators reported that despite having basic cybersecurity frameworks in place, over 70% of institutions lacked regular cybersecurity training programs for students and staff, contributing to the high incidence of cyber threats such as phishing and online extortion.

Therefore, these interviews played a critical role in triangulating the findings, deepening the understanding of institutional gaps, and informing targeted recommendations for improving cybersecurity resilience in tertiary institutions. This observation echoes the findings of Aliyu et al. (2020), who identified weak institutional frameworks as a barrier to effective cybersecurity implementation in educational institutions. The findings are also in agreement with those in a study by Wanjiru et al. (2023), who found that varying awareness levels among students directly affect their understanding of institutional commitments to cybersecurity in Kenya.

An unexpected result was the relatively low engagement of students with cybersecurity training programs, despite institutions offering such initiatives. This suggests that while awareness campaigns exist, their effectiveness in encouraging participation may be limited by inadequate outreach strategies or student apathy toward cybersecurity issues. Addressing these gaps through targeted training and institution-wide communication strategies will be essential for improving cybersecurity resilience in academic settings.

5.2.2 Incidence of Cybersecurity Threats Experienced by Students

The findings in Section 4.3.3 reveal a notable incidence of cybersecurity threats among students in Nakuru County's tertiary institutions. A majority of respondents agreed or strongly agreed that they had encountered fraudulent attempts to obtain sensitive information, malicious software, and manipulative tactics such as social engineering, with mean scores ranging around 3.79 across items. This indicates that cyber threats such as phishing and malware infections are not isolated events but rather frequent occurrences, aligning with studies by Khan et al. (2022) and Mensah and Asante (2023) that documented similar vulnerabilities among students in other regions. The high level of exposure underscores an urgent need for institutions to strengthen cybersecurity infrastructure and educational interventions. The finding also resonates with Ntaganda's (2018) observations in Rwanda, where manipulative cyber techniques were prevalent among students. Collectively, the results paint a picture of a digital environment fraught with significant risks to students' academic and personal security.

Moreover, students expressed substantial concern regarding the frequency of cyber threats, with a combined 62.7% indicating agreement or strong agreement with such worries. This heightened perception of risk suggests an increasing awareness of cybersecurity issues among students, which is supported by findings from Jawaid (2023), who also noted growing concern among students during the transition to remote learning environments. Despite awareness, a significant proportion of students remained neutral regarding their institutions' technological defenses, raising questions about the visibility and effectiveness of firewalls, antivirus software, and other cybersecurity measures. Mugisha (2020) similarly reported that limited technical capacity in institutions hampers effective cyber

defense efforts. The disparity between perceived threat and confidence in institutional protection mechanisms highlights a critical gap that requires immediate institutional attention. It points to the necessity of not only installing technological defenses but also ensuring their effectiveness and communicating these efforts clearly to students.

Lastly, the data reveal mixed levels of personal knowledge on how to protect against cyber threats, with 59.5% of students agreeing or strongly agreeing that they know how to safeguard themselves, while a notable minority felt less confident. This discrepancy emphasizes the need for continuous and targeted cybersecurity training programs to enhance students' self-efficacy. As emphasized by Badamasi and Utulu (2021), consistent cybersecurity education is vital for fostering resilient digital behaviors among students. The results also echo findings by Gabra et al. (2022), who identified a need for ongoing awareness initiatives to build stronger institutional cybersecurity cultures. Without regular training and proactive institutional engagement, students remain vulnerable to exploitation, even if basic cybersecurity measures are in place. Overall, the findings stress that protecting students in digital spaces requires an integrated approach combining technological defenses, education, and institutional transparency.

5.2.3 Preparedness of Diverse Tertiary Institutions

Institutional preparedness to counter cybersecurity threats varied across the surveyed tertiary institutions. The findings indicate that while some institutions have established technological defenses such as firewalls and antivirus software, the adequacy and effectiveness of these measures remain uncertain. This aligns with the Technology Acceptance Model (TAM), which suggests that the perceived usefulness and ease of use of security technologies influence their adoption and effectiveness (Davis, 1989). In this case, institutions may need to enhance cybersecurity infrastructure while simultaneously ensuring that students and staff are adequately trained to utilize these resources effectively.

The interviews conducted with student leaders and institutional security administrators revealed critical insights into the current state of cybersecurity preparedness within Nakuru County's tertiary institutions. One of the key findings was a strong positive correlation

between institutional preparedness and the creation of a secure learning environment (Table 4.12)

. Institutions that demonstrated higher levels of threat recognition, cybersecurity policy awareness, and access to training resources also reported lower incidences of cyber-attacks among their students. This finding supports Mugisha (2020), who emphasized that institutions with well-developed cybersecurity frameworks experienced fewer incidents and fostered greater digital confidence among students. However, despite this progress, interviews revealed that many institutions still employed reactive approaches to cybersecurity, waiting until after an incident occurred to take preventive measures. This reactive culture exposes students to preventable risks and highlights the urgent need for more proactive threat identification systems and preventive cybersecurity strategies.

Another significant observation from the interviews was the disparity in cybersecurity preparedness between public and private institutions. Private universities generally reported greater investments in cybersecurity infrastructure, training programs, and regular policy updates compared to their public counterparts. In contrast, public institutions cited frequent challenges such as limited budgets, bureaucratic delays, and minimal allocation of resources to cybersecurity initiatives. This disparity not only reflects differences in institutional priorities but also raises concerns about the growing digital divide in cybersecurity resilience among students depending on the type of institution they attend. Similar to the findings of Mugisha (2020) in Rwanda, public institutions often lacked the technical capacity to implement advanced cybersecurity measures effectively, leading to higher vulnerability rates. Therefore, the results point to an urgent need for policy interventions aimed at enforcing uniform minimum cybersecurity standards across both public and private institutions to ensure equitable protection for all students.

The study further highlighted the necessity for more transparent and standardized operational practices in cybersecurity management across tertiary institutions. Interviews with Information Security Officers revealed inconsistencies in the communication of cybersecurity policies, threat reporting protocols, and resource allocation within institutions, particularly among public universities. Without transparent and clearly

communicated cybersecurity procedures, students remained unaware of best practices, leaving them vulnerable to cyber-attacks such as phishing and online extortion. Mugisha's (2020) findings similarly underscored that the lack of technical resources and systematic operational frameworks severely limited the success of cybersecurity initiatives in Rwanda. In Nakuru County, the results suggest that enhancing transparency, institutional accountability, and student involvement in cybersecurity initiatives could significantly bolster the resilience of the learning environment. Therefore, it is imperative that institutions not only invest in infrastructure but also embed cybersecurity practices within their organizational culture, making cybersecurity awareness and preparedness a routine part of campus life.

The study findings provide critical insights into the intersection between cybersecurity awareness, threat experiences, and institutional preparedness in Kenya's tertiary institutions. The application of Protection Motivation Theory (PMT), Routine Activity Theory, and the Technology Acceptance Model (TAM) reinforces the argument that cybersecurity awareness alone is insufficient; effective security frameworks require active institutional involvement, technological adoption, and behavioral change among students.

Addressing the gaps identified in this study will require a multi-faceted approach, including enhanced cybersecurity education, institutional investment in security infrastructure, and the development of national cybersecurity policies tailored to educational institutions. The study also underscores the need for further research into behavioral cybersecurity interventions that move beyond awareness and focus on practical skills development among students. Without such interventions, the risk of cyber threats in Kenya's tertiary institutions is likely to escalate, posing significant risks to academic integrity and personal security in an increasingly digitalized education landscape.

5.3 Summary of Findings

5.3.1 Extent of Awareness of Cybersecurity Policies

The findings reveal a moderate level of awareness regarding cybersecurity policies among tertiary institution students in Nakuru County, Kenya, with a notable percentage

demonstrating familiarity with various policies, such as data protection and acceptable use policies. However, significant gaps persist in understanding and training related to these policies, highlighting a need for ongoing educational efforts and improved institutional communication. Students expressed a fair degree of awareness regarding whom to contact in case of a data breach, indicating a proactive stance on immediate actions during cybersecurity incidents. The analysis also shows a strong positive correlation between awareness of cybersecurity policies and the establishment of secure learning environments, suggesting that enhancing students' understanding is essential for fostering safety within academic settings. Overall, addressing the identified gaps in training and communication will be crucial for developing a secure educational landscape in an increasingly digital environment. The extent of awareness of cybersecurity policies shows a significant positive effect ($\beta = .257$, $p < .001$), suggesting that increased awareness is a crucial factor in enhancing security.

5.3.2 Incidence of Cyber Security Threats Experienced by students

The findings indicate that a significant proportion of students in Nakuru County's tertiary institutions have encountered various cybersecurity threats, including fraudulent attempts to obtain sensitive information, malicious software, and manipulative techniques to deceive them into divulging confidential information. The majority of students expressed concerns about the frequency of these threats, and there is a general recognition of the technological solutions implemented by institutions, although perceptions of their effectiveness vary. Additionally, while many students believe they know how to protect themselves from cyber threats, there remains a need for enhanced cybersecurity education to bolster their resilience. The strong positive correlation ($r = 0.863$) between the incidence of cybersecurity threats and the creation of a secure learning environment suggests that effectively addressing these threats is crucial for fostering a safer academic environment in Kenyan tertiary institutions. The Incidence of Cyber Security Threats Experienced by students has a strong positive influence ($\beta = .310$, $p < .001$), indicating that students' experiences with threats drive the need for a secure environment.

5.3.3 Preparedness of Diverse Tertiary Institutions

The findings reveal that a significant portion of respondents in Nakuru County's tertiary institutions have encountered various cybersecurity threats, such as fraudulent attempts to obtain sensitive information, malicious software, and manipulative techniques. A notable percentage expressed concerns about the frequency of these threats, highlighting the need for enhanced institutional support and cyber hygiene programs. Although many respondents believe their institutions employ technological solutions like firewalls and antivirus software, there is still uncertainty about the effectiveness of these measures, with a considerable number remaining neutral. Furthermore, while some respondents feel confident in their ability to protect themselves from cyber threats, there remains a critical minority who do not share this confidence, underscoring the need for regular cybersecurity training. The strong positive correlation ($r = 0.848$, $p = 0.000$) between institutional preparedness and the creation of a secure learning environment suggests that improving readiness through enhanced cybersecurity infrastructure and staff training significantly contributes to the security of the academic environment. These findings align with previous studies emphasizing the importance of robust cybersecurity measures and preparedness in educational institutions. Preparedness of Diverse Tertiary Institutions ($\beta = .228$, $p < .001$) is significant.

5.4 Conclusions

The study concludes that enhancing awareness of cybersecurity policies among students in Nakuru County's tertiary institutions is crucial for creating a secure learning environment. While there is a moderate level of awareness, significant gaps in understanding and training persist. These gaps hinder the effective implementation of cybersecurity measures. Therefore, institutions must prioritize ongoing educational efforts and improved communication to ensure students are well-informed about cybersecurity policies and the steps to take in the event of a cyber incident. The positive impact of cybersecurity policy awareness on security underscores the importance of this initiative.

Furthermore, the study highlights the pervasive nature of cybersecurity threats experienced by students, including fraudulent activities, malicious software, and manipulative

techniques. The widespread exposure to these threats has raised concerns among students and emphasized the need for robust cybersecurity education and institutional support. The strong correlation between the incidence of cybersecurity threats and the creation of a secure learning environment suggests that addressing these threats effectively is vital for maintaining a safe academic environment. Institutions must invest in both technological solutions and comprehensive training programs to enhance students' resilience against these threats.

Lastly, the preparedness of diverse tertiary institutions in Nakuru County plays a critical role in fostering a secure academic environment. While many respondents believe their institutions are equipped with technological solutions, there remains skepticism about their effectiveness. The need for regular cybersecurity training and improved infrastructure is evident, as significant minorities of students do not feel adequately prepared to protect themselves from cyber threats. The strong correlation between institutional preparedness and a secure learning environment underscores the importance of investing in cybersecurity infrastructure, staff training, and proactive threat management strategies. This investment is essential for ensuring the safety and security of students and staff in an increasingly digital educational landscape.

5.5 Recommendations

Based on the findings, the study recommends as follows.

5.5.1 Recommendations for Policymakers

Policymakers play a crucial role in shaping the cybersecurity landscape within tertiary institutions. Based on the study findings, it is recommended that national education and ICT regulatory bodies develop and enforce comprehensive cybersecurity policies tailored specifically for academic institutions. These policies should mandate the inclusion of cybersecurity awareness programs within the curricula of tertiary institutions, ensuring that students are adequately prepared to navigate digital threats. Additionally, funding allocations for cybersecurity infrastructure and training should be increased, particularly for public institutions that face financial constraints. Collaborating with international

cybersecurity organizations and industry experts can also provide insights into best practices that can be localized for the Kenyan education sector.

5.5.2 Recommendations for Educators

Educators serve as primary agents in disseminating cybersecurity knowledge and fostering awareness among students. To enhance cybersecurity education, it is recommended that institutions integrate cybersecurity training into various academic programs, rather than limiting it to IT-related courses. This interdisciplinary approach will ensure that students across all disciplines develop essential cybersecurity skills. Moreover, educators should employ interactive teaching methodologies such as simulated cyber-attack scenarios, workshops, and real-world case studies to make cybersecurity training more practical and engaging. Faculty development programs should also include cybersecurity training to ensure that lecturers and instructors are well-equipped to teach and reinforce cybersecurity best practices.

5.5.3 Recommendations for IT Administrators

IT administrators are responsible for ensuring that cybersecurity measures are effectively implemented within tertiary institutions. To enhance institutional preparedness, IT departments should establish proactive threat detection mechanisms, such as continuous network monitoring and real-time security alerts. Institutions should also invest in multi-layered cybersecurity defenses, including firewalls, anti-malware programs, and encryption technologies. Furthermore, IT administrators must implement routine cybersecurity drills and penetration testing to assess and strengthen institutional defenses. User training programs should be conducted regularly to ensure that students and faculty understand security protocols and recognize potential threats.

5.5.4 Recommendations for Students

Students must take an active role in their own cybersecurity awareness and behavior. It is recommended that student organizations collaborate with IT departments to organize peer-led cybersecurity workshops and campaigns. Institutions should also create accessible

cybersecurity resource centers where students can access educational materials, toolkits, and guidance on safe online practices. Additionally, students should be encouraged to adopt secure habits such as using multi-factor authentication, regularly updating passwords, and being cautious of phishing attempts. Integrating cybersecurity awareness into student orientation programs can also ensure that new students develop security-conscious habits from the outset of their academic journey.

5.5.5 Recommendations for Institutional Leadership

Institutional leaders, including university administrators and decision-makers, must prioritize cybersecurity as a fundamental component of educational excellence. It is recommended that institutions establish dedicated cybersecurity task forces responsible for developing, implementing, and reviewing cybersecurity strategies. Leadership should also allocate sufficient financial resources to cybersecurity initiatives, including staff training, infrastructure improvements, and awareness programs. Regular cybersecurity audits should be conducted to assess compliance with best practices and identify areas for improvement. Additionally, institutions should foster partnerships with private sector organizations, government agencies, and cybersecurity firms to access expertise and resources that can strengthen institutional cybersecurity measures.

5.6 Areas for Further Studies

Future research should consider exploring the role of cybersecurity policies in other counties across Kenya to determine if the trends observed in Nakuru County are consistent nationwide. Such a study could provide comparative insights and help identify regional disparities in cybersecurity awareness and preparedness, guiding targeted interventions.

Additionally, it would be beneficial to conduct longitudinal studies to assess the long-term effectiveness of cybersecurity training programs in tertiary institutions. By tracking changes in students' awareness, behavior, and the incidence of cyber threats over time, researchers could evaluate the sustained impact of these programs and identify areas for improvement.

Lastly, further studies should investigate the influence of emerging technologies, such as artificial intelligence and blockchain, on cybersecurity in educational institutions. Understanding how these technologies can be leveraged or potentially exploited within the academic environment could offer new perspectives on enhancing security measures and preparing institutions for future challenges.

REFERENCES

Adekunle, O. J., et al. (2020). Enhancing Cybersecurity Awareness among Students in Tertiary Institutions: A Case Study of Nigerian Universities. *Journal of Cybersecurity Education, 5*(2), 78-92.

Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. Journal of King Saud University - Computer and Information Sciences, 34(10), 8176-8206.

Alharbi, T., & Tassaddiq, A. (2021). Assessment of Cybersecurity Awareness among Students of Majmaah University. *Big Data and Cognitive Computing, 5*(2), 23. https://doi.org/10.3390/bdcc5020023

Al Shabibi, A.M., Al-Suqri, M.N. (2023). *Cybersecurity Awareness Among Students During the COVID-19 Digital Transformation of Education: A Case Study at the Muscat (Oman) Schools.* In: Al Naimiy, H.M.K., Bettayeb, M., Elmehdi, H.M., Shehadi, I. (eds) Future Trends in Education Post COVID-19. SHJEDU 2022. Springer, Singapore. https://doi.org/10.1007/978-981-99-1927-7_4

Aliyu, A., Aliyu, M., Ahmad, A., & Abdullahi, S. (2021). Investigating cybersecurity awareness among tertiary institutions students in Nigeria. *International Journal of Advances in Engineering and Management (IJAEM), 3*(10), 111-118.

Alqahtani, M. A. (2022). Factors Affecting Cybersecurity Awareness among University Students. *Applied Sciences, 12*(5):2589. https://doi.org/10.3390/app12052589

Badamasi, B. & Utulu, S. (2021). *Framework for Managing Cybercrime Risks in Nigerian Universities*. Proceedings of the 1st Virtual Conference on Implications of Information and Digital Technologies for Development. Amrican University of Nigeria

Bandura, A. (1977). *Social learning theory*. Prentice-Hall.

Bordonaba-Juste, M. aV, Lucia-Palacios, L., & Pérez-López, R. (2020). Generational differences in valuing usefulness, privacy and security negative experiences for paying for cloud services. *Information Systems and E-Business Management, 18*(1), 35–60.10.1007/s10257-020-00462-8

Bottyán, L. (2023). Cybersecurity awareness among university students. *Journal of Applied Technical and Educational Sciences, jATES, 13*(3), 1-11

Bryman, A. (2022). *Social research methods* (6th ed.). Oxford University Press.

Cardwell, A. (2024). *Beyond Security Awareness: 2024 Cybersecurity Fun and Games.* https://www.linkedin.com/pulse/beyond-security-awareness-2024-cybersecurity-fun-games-cardwell-xsnac/

Cheng, E. C. K & Wang, T. (2022). Institutional Strategies for Cybersecurity in Higher *Education Institutions. Information. 2022; 13*(4):192. https://doi.org/10.3390/info13040192

Chizanga, M. K. Agola, J. Rodrigues, A. (2022). factors affecting cyber security awareness in combating cybercrime in Kenyan public universities, Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET, 6*(1), pp 54-57, January 2022. Article DOI https://doi.org/10.47001/IRJIET/2022.601011

Cohen, L., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588-608

Communications Authority of Kenya. (2022). *Report on cybercrime cases targeting tertiary institution students.* Retrieved from https://files.eric.ed.gov/fulltext/EJ1348600.pdf.

Creswell, J. W., & Creswell, J. D. (2023). *Research design: Qualitative, quantitative, and mixed methods approaches* (6th ed.). SAGE Publications.

Daengsi, T., Pornpongtechavanich, P., & Wuttidittachotti, P. (2022). Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai

Employees Associated with Phishing Attacks. *Education and Information Technologies, 27*(4), 4729-4752. https://doi.org/10.1007/s10639-021-10806-7

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-340.

Gabra, A., Sirat, M., Hajar., & Dauda, I. (2022). Cyber security awareness among university students: A case study. *Science Proceedings Series 2*(1), 82 - 86

Gkrimpizi T, Peristeras V, Magnisalis I. (2023). Classification of Barriers to Digital Transformation in Higher Education Institutions: *Systematic Literature Review. Education Sciences 13*(7):746. https://doi.org/10.3390/educsci13070746

Jawaid, S. (2023). Cyber security threats to educational institutes: A growing concern for the new era of cybersecurity. *International Journal of Data Science and Big Data Analytics 2*(2), DOI:10.51483/IJDSBDA.2.2.2022.11-17

Jones, A. (2023). It *was everywhere all at once": Exploring Digital Coercive Control in the Context of Intimate Partner Violence through Mix Method Research.* The University Of New Brunswick

Jones, A. B., & Brown, C. D. (2020). Understanding Students' Awareness of Cybersecurity Policies in Higher Education Institutions. *Journal of Educational Technology*, 12(3), 45-58.

Khan, S. A., et al. (2022). Assessing Students' Awareness of Cybersecurity Policies in Higher Education: A Case Study of Pakistani Universities. *Journal of Information Security Education*, 8(1), 112-127.

Karatas, K. (2020). *The Competencies of the Culturally Responsive Teacher: What, Why and How?. i.e.: inquiry in education*: Vol. 12: Iss. 2, Article 2. Retrieved from: https://digitalcommons.nl.edu/ie/vol12/iss2/2

Kenya National Examinations Council. (2023). *Academic dishonesty and cyber security awareness among tertiary students*. Unpublished raw data. https://ir-library.ku.ac.ke/handle/123456789/26696

KPMG China (2016). *Cyber security in China.* Available at https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2016/08/cyber-security-in-china.pdf

Li, Y. & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports, 7,* 8176-8186

Makulec, A., & Dlamini, B. (2021). Effectiveness of Cyber Security Awareness Campaigns in South Africa. *Journal of Cybersecurity Awareness, 1*0(2), 45-58.

Mensah, K., & Asante, G. (2023). Perceptions of Cybersecurity Policies among Tertiary Institution Students in Ghana. *Journal of Cybersecurity Awareness*, 16(4), 220-235.

Moallem, A. (2019). *Cyber Security Awareness Among College Students" Advances in Human Factors in Cybersecurity.* AHFE 2018. Advances in Intelligent Systems and Computing, 79-87. doi:10.1007/978-3-319-94782-2_8

Mthombeni, S., & Mthombeni, T. (2020). Assessing Cyber Threat Readiness in South African Organizations. *International Journal of Cybersecurity Policy and Resilience Studies, 8*(1), 32-45.

Mugisha, T. (2020). Cybersecurity awareness and institutional preparedness in African universities. *African Journal of Information Security, 5*(1), 98-121.

Ntaganda, N. (2018). *Cyber Security Awareness in Rwanda.* National University of Uganda.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93-114.

Safitra, M. F, Lubis, M., & Fakhrurroja, H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. *Sustainability, 15*(18):13369. https://doi.org/10.3390/su151813369

Saleem, H., Khan, M. A., & Zafar, S. (2021). The role of cybersecurity training in higher education institutions: An analysis of Pakistan. *Computers & Security, 45*(3), 156-174.

Smith, J. R., et al. (2021). Exploring Cybersecurity Policy Awareness among University Students in the UK. *International Journal of Cybersecurity Research*, 3(2), 55-68.

Taber, K. S. (2020). The use of Cronbach's Alpha when developing and reporting research instruments in science education. *Research in Science Education, 50*(1), 1-24. https://doi.org/10.1007/s11165-019-09978-4

Taherdoost, H. (2022). Validity and reliability of research instruments: Conceptual and practical considerations. *Journal of Management Research, 14*(1), 1-15. https://doi.org/10.1007/s40685-022-00261-4

Tan, L. K., & Lim, S. H. (2021). Promoting Cybersecurity Awareness among Tertiary Students in Malaysia: Strategies and Challenges. *Journal of Educational Technology and Society*, 24(3), 87-101.

Tavakol, M., & Dennick, R. (2021). Making sense of Cronbach's Alpha. *International Journal of Medical Education, 2*(1), 53-55. https://doi.org/10.5116/ijme.4dfb.8dfd

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

Wang, X. (2022). Exploring Chinese college students' awareness of information security in the COVID-19 era. *European Journal of Education, 5*(2), 21 - 54

Wanjiru, M., Kamau, J., & Njoroge, P. (2023). Evaluating cybersecurity frameworks in Kenyan tertiary institutions. *Kenyan Journal of ICT Security, 8*(2), 140-160.

Zhang, L., Wang, H., & Li, Y. (2022). Cyber Security Awareness Policies in China: A Comprehensive Analysis. *Chinese Journal of Cybersecurity, 8*(1), 45-62.

Zulkifli, Z., Abdul Molok, N. N., Abd Rahim, N. H., & Talib, S. (2020). Cyber Security Awareness Among Secondary School Students in Malaysia. *Journal of Information Systems and Digital Technologies*, *2*(2), 28–41. https://doi.org/10.31436/jisdt.v2i2.151

APPENDICES

Appendix 1: Research Questionnaire for Students

Your participation in this questionnaire will contribute invaluable insights to our study on the role of influencers in community development in Kenya.

Part A: Demographic Characteristics

1. Gender

   Male [ ] Female [ ]

2. Age in Years

   16-25 [ ]

   26-35 [ ]

   36-45 [ ]

   46-55 [ ]

   56+ [ ]

3. Study level

   Certificate [ ]

   Diploma [ ]

   Bachelor's Degree [ ]

   Master's Degree [ ]

   PhD, Other [ ]

4. Have you or any of your friends been a victim of any cybercrime?

   Femicide [ ]

   Exam cheating, [ ]

   Social media abuses [ ]

   Recruitment into extremist groups via social platforms [ ]

   Extortion [ ]

   Hacking [ ]

Part B: Extent of Awareness of Cybersecurity Policies

1. The following statements relate to extent of awareness of cybersecurity policies. Please indicate your level of agreement using a 5-point Likert scale where 1=Strongly Disagree, 2=Disagree, 3=Neutral, 4=Agree, and 5=Strongly Agree.

No	Statement	1	2	3	4	5
1	I am aware of the data protection policy at my institution.					
2	I understand the key elements of the network security policy.					
3	I am familiar with the data acceptable use policy.					
4	I have received training on data protection policies.					
5	The institution regularly updates us on cybersecurity policies.					
6	I know whom to contact in case of a data breach.					

Part C: Incidence of Cyber Security Threats Experienced by students

2. The following statements relate to incidence of cyber security threats experienced. Please indicate your level of agreement using a 5-point Likert scale where 1=Strongly Disagree, 2=Disagree, 3=Neutral, 4=Agree, and 5=Strongly Agree.

No	Statement	1	2	3	4	5
1	I have encountered fraudulent attempts to obtain sensitive information in the past					
2	I have encountered Malicious software designed to disrupt, damage, or gain unauthorized access to my computer systems					
3	I have encountered manipulative techniques used to deceive individuals into divulging confidential information or performing					
4	I am concerned about the frequency of cyber threats					

5	The institution likely employs a range of technological solutions, such as firewalls, antivirus software					
6	I believe cyber threats are adequately addressed in my institution					

Section D: Preparedness of Diverse Tertiary Institutions

3. The following statements relate to preparedness of diverse tertiary institutions. Please indicate your level of agreement using a 5-point Likert scale where 1=Strongly Disagree, 2=Disagree, 3=Neutral, 4=Agree, and 5=Strongly Agree.

	Statement	1	2	3	4	5
1	I can recognize potential cybersecurity threats.					
2	I have a good understanding of cyber risks.					
3	I am confident in my institution's ability to manage cybersecurity threats.					
4	My institution provides sufficient resources for cybersecurity preparedness.					
5	I believe the cybersecurity measures in place are adequate.					
6	I am aware of the steps to take during a cybersecurity incident.					

Part E: Access to Cybersecurity Education

4. The following statements relate to access to cybersecurity education. Please indicate your level of agreement using a 5-point Likert scale where 1=Strongly Disagree, 2=Disagree, 3=Neutral, 4=Agree, and 5=Strongly Agree.

No	**Statement**	**1**	**2**	**3**	**4**	**5**
1	Cybersecurity is integrated into my curriculum.					

2	There are adequate resources available for learning about cybersecurity.					
3	I receive regular training on cybersecurity.					
4	I have access to up-to-date cybersecurity tools for learning.					
5	My institution encourages participation in cybersecurity workshops.					
6	Cybersecurity education is a priority at my institution.					

Section F: Creation of a Secure Learning Environment

5. The following statements relate to creation of a secure learning environment. Please indicate your level of agreement using a 5-point Likert scale where 1=Strongly Disagree, 2=Disagree, 3=Neutral, 4=Agree, and 5=Strongly Agree.

No	**Statement**	**1**	**2**	**3**	**4**	**5**
1	I can identify cybersecurity risks in my learning environment.					
2	I understand the preventive measures to avoid cybersecurity threats.					
3	I recognize warning signs of potential cyber threats.					
4	My institution provides a secure online environment for learning.					
5	I feel confident using online resources without compromising security.					
6	My peers are also aware of the importance of cybersecurity.					

Thank you

Appendix II: Interview Schedule for Students

These questions aim to gather insights into students' awareness, experiences, and perceptions related to cyber security threats and incidents, as well as their knowledge of institutional policies and resources available for cyber security education and training.

Part 1: Extent of Awareness of Cybersecurity Policies

1. Can you describe your understanding of the cyber security policies implemented by your institution? (Policy Understanding Level)
2. How aware are you of the specific cyber security policies and guidelines set forth by your institution? (Institutional Policy Awareness)
3. Can you share any instances where you have observed or experienced non-compliance with cyber security policies among students? (Policy Compliance Rate)

Part 2: Students' Awareness of Common Cyber Threats

1. How confident are you in recognizing common cyber threats such as phishing emails or malware attacks? (Threat Recognition Rate)
2. What is your level of knowledge regarding the potential risks associated with online activities, such as sharing personal information or downloading files? (Knowledge of Cyber Risks)
3. How seriously do you perceive the threat of cyber-attacks and online security breaches in your day-to-day life? (Threat Perception Level)

Part 3: Incidence of Cyber Security Threats Experienced

1. Have you personally encountered any cyber security threats or attacks while using digital devices or online platforms? If so, could you describe the nature of these incidents? (Threat Encounter Frequency)
2. Can you recall any specific instances where you or someone you know has been the victim of a cyber-attack or security breach? (Cyber Attack Incidence)
3. How likely do you think students are to report cyber security incidents or breaches to the relevant authorities? (Threat Incident Reporting)

Part 4: Knowledge of Peers Victimized by Cyber Security Threats

1. Are you aware of any of your peers who have been targeted or victimized by cyber security threats? (Peer Victimization Awareness)
2. Have you or your peers ever discussed incidents involving cyber security breaches or attacks within your academic or social circles? (Peer Incident Awareness)
3. How effective do you think students are in identifying and reporting instances of cyber security threats affecting their peers? (Victim Identification Rate)

Part 5: Access to Cybersecurity Education

1. How integrated do you feel cyber security education is within your academic curriculum? (Curriculum Integration Level)
2. In your opinion, what resources are currently available to students to enhance their understanding of cyber security concepts and practices? (Availability of Resources)
3. How frequently are students provided with training or workshops on cyber security awareness and best practices? (Frequency of Training)

Part 6: Level of Cyber Security Threat Awareness among Students

1. Can you identify some of the most common risks associated with using the internet and digital devices for academic and personal purposes? (Identification of Risks)
2. How well do you understand the preventive measures and strategies recommended to mitigate cyber security threats, such as using strong passwords or enabling two-factor authentication? (Understanding Preventive Measures)
3. Do you feel confident in your ability to recognize warning signs indicating a potential cyber security threat or attack, such as suspicious emails or unusual website behaviors? (Recognition of Warning Signs)

Appendix III: Interview Schedule for Security Administrators:

1. Can you describe the current cybersecurity policies and protocols in place at your institution?
2. How are these cybersecurity policies communicated to students and faculty members?
3. In your opinion, how effective are these policies in raising awareness about cybersecurity among students?
4. What measures does your institution take to ensure students are adequately trained on cybersecurity best practices?
5. Have you observed any common cyber threats or security breaches affecting students in your institution?
6. How does your institution monitor and detect potential cybersecurity incidents?
7. What steps are taken to respond to and mitigate cybersecurity incidents once they are detected?
8. Are there any particular challenges or obstacles your institution faces in maintaining cybersecurity for students?
9. How do you collaborate with other departments or external stakeholders to address cybersecurity concerns?
10. In your view, what additional measures or resources could improve cybersecurity awareness and preparedness among students in tertiary institutions?

Appendix IV: Sampled Tertiary Institutions in Nakuru County, Kenya

Tertiary Institution	Type	Estimated Student Population
African Institute of Research and Development Studies - Nakuru Town Campus	College	3000
Institute of Advanced Technology - Nakuru Campus	College	1000
Kenya Institute of Development Studies - Naivasha Campus (Oserian Estate)	College	1000
Kenya Medical Training College - Nakuru Campus	College	2000
Kenya Wildlife Service Training Institute - Main campus	College	1000
Nairobi Aviation College - Nakuru Campus	College	1000
Kabarak University - Main Campus	Private University	3,000
Kabarak University - Nakuru Town Campus	Private University	1000
Kenya Methodist University - Nakuru Campus	Private University	2000
Mount Kenya University - Nakuru Campus (MKU Annex)	Private University	1000
Egerton University - Nakuru Town Campus	Public University	3,500
Egerton University - Njoro Campus	Public University	10000
Jomo Kenyatta University of Agriculture and Technology - Nakuru Center	Public University	1,000
Kenyatta University - Nakuru Campus	Public University	1000
Laikipia University - Naivasha Campus	Public University	1000

Kenya Industrial Training Institute - Nakuru (Solai Road)	TVET	1000
Nakuru Training Institute – Nakuru	TVET	800
Rift Valley Institute of Science and Technology - Main Campus	TVET	4000
Rift Valley Institute of Science and Technology - Town Campus	TVET	1000
Sensei Institute of Technology – Nakuru	TVET	500
Estimate population		**39,800**

Appendix V: Letter of Introduction from the University

AFRICA NAZARENE
UNIVERSITY

P.O.Box: 53067 – 00200
Nairobi, Kenya.
Tel: 020 252 7170/1 – 5
Email: vc@anu.ac.ke
www.anu.ac.ke

23rd May 2024

RE: TO WHOM IT MAY CONCERN

Shadrack Toroitich Lomatong (19S01DMGP007) is a bonafide student at Africa Nazarene University. He has finished his course work and has defended his thesis proposal

entitled: -

"Exploring the role of Cyber Security Threat Awareness on Creation of a Secure Learning Environment in Kenya's Tertiary Institutions: A Case of Nakuru County.

Any assistance accorded to him to facilitate data collection and finish his thesis is highly welcomed.

Rodney J. Reed

Prof. Rodney Reed
Deputy Vice Chancellor, Academic & Student Affairs

Appendix VI: Research Permit

REPUBLIC OF KENYA

NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Ref No: **963291**

Date of Issue: **31/May/2024**

RESEARCH LICENSE

This is to Certify that Mr.. Shadrack Toroitich Toroitich of Africa Nazarene University, has been licensed to conduct research as per the provision of the Science, Technology and Innovation Act, 2013 (Rev.2014) in Nakuru on the topic: EXPLORING THE ROLE OF CYBER SECURITY THREAT AWARENESS ON CREATION OF A SECURE LEARNING ENVIRONMENT IN KENYA'S TERTIARY INSTITUTIONS: A CASE OF NAKURU COUNTY for the period ending : 31/May/2025.

License No: **NACOSTI/P/24/36544**

963291

Applicant Identification Number

Director General
NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Verification QR Code

NOTE: This is a computer generated License. To verify the authenticity of this document, Scan the QR Code using QR scanner application.

See overleaf for conditions

Appendix VII: Map of Nakuru County