Original Article
ISSN (Online): 3048-894X

Journal of Digital Security and Forensics
July-December 2025 2(2), 11–37

AN EVALUATION OF CYBER INCIDENT MANAGEMENT SYSTEMS IN HIGHER EDUCATION INSTITUTIONS (HEIS) IN KENYA

Paul Okanda [1], Abdijabar Abass [2]

[1] Associate Professor, Computing and Informatics Department, School of Science & Technology, United States International University-Africa, Kenya
[2] Graduate, Computing and Informatics Department, School of Science and Technology, United States International University-Africa, Kenya

Received 28 August 2025
Accepted 29 September 2025
Published 07 October 2025

Corresponding Author

Paul Okanda, pokanda@usiu.ac.ke

DOI
10.29121/DigiSecForensics.v2.i2.2025.50

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

Kenyan universities are increasingly integrating digital technologies into their academic and administrative operations. However, this digital transformation has exposed institutions to escalating cybersecurity threats, including data breaches, ransomware attacks, and unauthorized access to critical information. This study evaluates the effectiveness of existing cybersecurity measures in Kenyan universities, aiming to identify key vulnerabilities and areas for improvement. A structured survey was conducted among IT personnel from four major Kenyan universities, gathering data on cybersecurity preparedness, existing frameworks, and incident response strategies. The findings indicate that while universities have implemented foundational cybersecurity controls such as firewall systems and access controls, there are significant gaps in real-time threat detection, incident response preparedness, and cybersecurity training programs. Majority of institutions lack dedicated cybersecurity teams, and incident response mechanisms are largely reactive rather than proactive. Additionally, limited financial and technical resources hinder effective implementation of cybersecurity policies. The study highlights critical deficiencies in cybersecurity frameworks currently in use and emphasizes the need for real-time monitoring systems, improved staff training, and the adoption of automated threat detection tools. The study recommends a multi-stakeholder approach involving universities, government agencies, and cybersecurity experts to enhance resilience against evolving cyber threats. Addressing these deficiencies is essential as it will enable Kenyan universities to strengthen their cybersecurity posture, protect academic assets, and safeguard the privacy of students and faculty members. This research contributes to ongoing discussions on cybersecurity in higher education and provides a foundation for developing more effective cybersecurity policies and frameworks in African academic institutions.

Keywords: Cybersecurity, Incident Management, Real-Time Threat Detection, Kenyan Universities, Cyber Threats

1. INTRODUCTION

In recent years, Kenyan universities have rapidly adopted digital technologies to support academic and administrative functions, Makori and Mauti (2016). The transition to cloud computing, online learning platforms, and digital libraries has significantly improved efficiency and accessibility. However, this digital shift has introduced considerable cybersecurity risks. Universities store vast amounts of sensitive student records, research data, financial transactions, and confidential administrative information, making them attractive targets for cybercriminals, Dolliver et al. (2021). The rising number of cyberattacks on higher education institutions globally and in Kenya underscores the urgent need for robust cybersecurity frameworks to protect critical academic assets, Owino (2025).

Cybersecurity threats against universities have evolved in complexity and frequency. Incidents such as data breaches, ransomware attacks, phishing scams, and denial-of-service (DoS) attacks have become more common in academic institutions worldwide. In Kenya, universities have reported cases of unauthorized access and theft of intellectual property, Musembi et al. (2024). The consequences of these security breaches are severe, including loss of academic integrity, financial implications, reputational damage, and disruptions in learning activities. Despite the growing cyber threats, most universities still rely on outdated security systems due to lack of investment as stated by Oprean et al. (2017).

One of the primary challenges in Kenyan universities is the lack of preparedness in their cybersecurity strategies. Most of them lack structured cybersecurity frameworks and do not have dedicated cybersecurity teams to manage incidents effectively. Additionally, staff and students often have minimal awareness of cybersecurity best practices, increasing the risk of social engineering attacks such as phishing and identity theft.

The Kenyan government has enacted laws and policies to promote cybersecurity, such as the Data Protection Act (2019), which mandates educational institutions to implement measures to safeguard personal data, Laibuta (2023). However, enforcement remains inconsistent across universities, and majority of institutions struggle to comply due to insufficient resources. This situation raises concerns about data privacy, regulatory compliance, and institutional resilience against cyber threats.

Globally, institutions have adopted established cybersecurity frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, National Institute of Standards and Technology. (2024), the MITRE ATT&CK Framework, Kim et al. (2023), and the Cyber Kill Chain Model, Hutchins et al. (2011), to strengthen their defense mechanisms. However, Kenyan universities have been slow to integrate these frameworks, often due to limited financial resources, lack of skilled cybersecurity professionals, and inconsistent enforcement of cybersecurity policies. Without an adequate real-time cyber threat detection system, universities remain exposed to evolving cyber threats.

This study seeks to assess the current cybersecurity strategies in Kenyan universities, focusing on identifying gaps in existing frameworks. By understanding the weaknesses in cybersecurity preparedness, this research provides valuable insights that can help universities enhance their cybersecurity posture, adopt real-time threat detection technologies, and implement effective incident response strategies. Addressing these gaps is crucial for protecting the integrity, confidentiality, and availability of academic resources and ensuring that Kenyan universities can operate securely in an evolving digital landscape.

Thus, this study is structured to evaluate cybersecurity measures, identify critical vulnerabilities, and provide recommendations for improving cybersecurity frameworks in Kenyan universities. By bridging these security gaps, institutions can mitigate risks, ensure compliance with data protection regulations, and safeguard their academic and research resources from cyber threats.

1.1. THE PROBLEM

Kenyan universities face heightened vulnerability to cyberattacks due to the lack of effective real-time threat detection and rapid response capabilities, despite efforts to improve cybersecurity awareness. This gap exposes institutions to risks such as data breaches, intellectual property theft, and reputational harm. Current cybersecurity measures are often showing a lack of preparedness, failing to address evolving threats effectively. The Kenyan Data Protection Act underscores the need for robust security measures to protect personal data, highlighting the urgency of developing tailored incident management frameworks to address these unique challenges.

1.2. PURPOSE OF THE STUDY

The primary objective of this study was to evaluate the cybersecurity measures currently in place at Kenyan universities. The main focus is on investigating the efficacy of existing cyber-security measures and the gaps in real-time threat detection and incident response mechanisms in Kenyan universities. The study aims to design a specialized incident management framework that aligns with the unique challenges and digital infrastructure of these institutions. Moreover, this research intends to provide actionable insights for universities to bolster their cyber-security posture against the evolving threat landscape.

2. LITERATURE REVIEW

The rise in cyber threats has led to an increased focus on cybersecurity in academic institutions. Universities worldwide have been targeted by cybercriminals due to the vast amounts of sensitive data they store, including student records, research findings, and financial information. Various studies have examined cybersecurity challenges in higher education, highlighting weaknesses in threat detection, incident management, and policy enforcement. In the context of Kenyan universities, several empirical studies have identified significant gaps in cybersecurity preparedness, emphasizing the urgent need for improved security measures.

Several studies Njoroge et al. (2021), Serem (2021), Kaibiru et al. (2023) consistently point to institutional weaknesses in cybersecurity awareness, incident response, and policy enforcement, although the degree and focus of these challenges vary across universities. It is notable that while Njoroge et al. (2021) focus on cybersecurity awareness in Kenyan universities, Chizanga et al. (2022) investigate the impact of financial resource constraints on cybersecurity infrastructure in African universities. Njoroge et al. (2021) conducted a study on cybersecurity awareness in Kenyan universities, revealing that a majority of faculty members and students lack basic knowledge of cybersecurity best practices. The study found that over 60% of cybersecurity incidents in universities result from human error, such

as falling for phishing scams or using weak passwords. Chizanga et al. (2022) investigated the impact of financial constraints on cybersecurity infrastructure in African universities. Their study found that limited budgets prevent universities from investing in critical security technologies such as firewalls, intrusion detection systems, and real-time threat monitoring tools. The researchers surveyed IT administrators from multiple institutions and discovered that only 30% of universities had dedicated cybersecurity budgets, while the rest relied on general IT funding, which often prioritized hardware and software procurement over security enhancements. The study emphasized that without adequate financial investment, universities remain highly exposed to cyber threats and are unable to implement comprehensive security frameworks.

Also, a study by Serem (2021) examined incident response mechanisms in Kenyan universities, assessing how institutions handle cybersecurity breaches while another study by study by Kaibiru et al. (2023) explored the role of policy enforcement in cybersecurity management. The study by Serem (2021) revealed that most universities lack structured incident response teams, and when security incidents occur, responses are often delayed or ineffective. Only 25% of universities surveyed had documented cybersecurity policies that outlined incident response procedures. The absence of dedicated response teams means that IT personnel often struggle to contain cyber threats, leading to prolonged system downtimes and potential data breaches. The study recommended the establishment of dedicated cybersecurity units within universities to improve response times and mitigate the impact of cyber incidents. On the other hand, Kaibiru et al. (2023) opine that while a large percentage of Kenyan universities have formal cybersecurity policies, enforcement remains weak due to a lack of accountability. Their findings indicated that universities often adopt generic cybersecurity policies without adapting them to their specific institutional needs. As a result, compliance levels are low, and security policies are rarely updated to reflect emerging threats. The study suggested that universities should establish independent cybersecurity oversight bodies to monitor compliance and ensure that security policies are effectively implemented and regularly reviewed.

Also, Maranga and Nelson (2019) compared cybersecurity practices in African and Western universities. Their research highlighted that universities in developed countries allocate significantly more resources to cybersecurity, leading to better preparedness and lower incident rates. For instance, institutions in the United States and Europe often have 24/7 security operations centers, dedicated cybersecurity teams, and advanced threat detection systems. In contrast, African universities, including those in Kenya, rely on outdated security tools and lack the human expertise needed to combat sophisticated cyber threats. The study emphasized that adopting global best practices, such as real-time threat intelligence sharing and continuous cybersecurity training, could help African universities strengthen their security posture.

Strom et al. (2018) analyzed the effectiveness of cybersecurity frameworks such as MITRE ATT&CK and the Cyber Kill Chain in higher education institutions. Their findings indicated that universities that implemented structured cybersecurity frameworks experienced fewer security breaches compared to those without formalized security strategies. However, in Kenya, the adoption of these frameworks remains low, with most universities lacking the technical expertise required for implementation. The study recommended collaboration between universities and industry experts to develop customized cybersecurity frameworks that align with the specific challenges faced by academic institutions.

Finally, a survey by Hutchins et al. (2011) assessed the application of the Cyber Kill Chain model in detecting cyber threats in universities. Their study found that institutions that actively mapped cyberattacks using this framework were able to identify threats earlier and respond more effectively. However, the study noted that most universities in Africa, including Kenya, do not use advanced threat detection models, instead relying on outdated security approaches. The researchers recommended that universities integrate real-time threat detection tools into their cybersecurity strategies to improve their ability to counter evolving cyber threats.

The following subsections present results from the analysis above, structured into key thematic areas. These include Cybersecurity Awareness and Awareness and Training; Resource Constraints and Infrastructure Gaps; Incident Management and Response Systems; Policy Enforcement and Institutional Oversight; and Adoption of Cybersecurity Frameworks.

2.1. CYBERSECURITY AWARENESS AND TRAINING

It is evident from the literature review above that despite the increasing number of cyberattacks targeting higher education institutions, most universities have not integrated cybersecurity training into their academic programs or staff development initiatives. The study concluded that improving cybersecurity awareness through regular training sessions could significantly reduce vulnerability to cyber threats.

2.2. RESOURCE CONSTRAINTS AND INFRASTRUCTURE GAPS

As analyzed above, implementing security frameworks can be resource intensive and most of the Kenyan universities may lack the necessary financial and human resources to fully implement these comprehensive cyber-security measures.

2.3. INCIDENT MANAGEMENT AND RESPONSE SYSTEMS

It is important that universities develop a coordinated response plan that includes stakeholder communication strategies. This involves creating incident response protocols, communication plans, and coordination mechanisms to ensure effective management of cybersecurity incidents. The Data Protection Act of Kenya mandates comprehensive measures to safeguard personal data, including the need for data controllers and processors to implement appropriate security measures to protect data against unauthorized access, loss, or damage Data Protection Act (2019). Therefore, the urgency of developing a tailored incident management framework and response systems requires strategic and informed interventions.

2.4. POLICY ENFORCEMENT AND INSTITUITIONAL OVERSIGHT

The impact of institutional policies on continuous monitoring suggests that strong governance, institutional oversight and policy enforcement significantly enhance continuous monitoring efforts. This implies that robust institutional policies are crucial for improving real-time monitoring of cybersecurity threats.

2.5. ADOPTION OF CYBERSECURITY FRAMEWORKS

One of the most significant gaps identified in the literature review is the inconsistency in the application and integration of cybersecurity measures across

different institutions. Although real-time monitoring systems were in place, they were not integrated with other security components, such as incident response protocols or access controls. This gap undermined the overall effectiveness of cybersecurity strategies, as individual systems were unable to communicate and respond cohesively to threats. The importance of integrated cybersecurity frameworks has been well-documented in the literature, with Fornell and Larcker (1981) arguing that the success of cybersecurity depends on the seamless interaction of multiple security layers to provide comprehensive protection.

A review of these empirical studies highlights several critical challenges facing Kenyan universities in cybersecurity management. First, there is a widespread lack of cybersecurity awareness among students and staff, making institutions vulnerable to phishing, ransomware, and other cyber threats. Second, financial limitations hinder the adoption of advanced security technologies, leaving universities reliant on outdated systems. Third, weak policy enforcement and a lack of dedicated cybersecurity personnel contribute to slow incident response times and ineffective threat mitigation strategies. Finally, the limited adoption of cybersecurity frameworks in Kenyan universities means that institutions do not benefit from structured approaches to managing cyber risks.

This empirical review underscores the urgency of improving cybersecurity in Kenyan universities. With increasing cyber threats targeting academic institutions, there is a critical need for comprehensive security measures that address vulnerabilities in awareness, funding, policy enforcement, and incident management.

2.6. THEORETICAL FRAMEWORKS

To further strengthen the theoretical foundation of this study, introduced are two pivotal theories: Protection Motivation Theory (PMT) and the Technology Acceptance Model (TAM). These theories are particularly relevant as they provide insights into the psychological and behavioral dimensions of cybersecurity practices, which are essential for the successful implementation of a real-time cyber threat detection framework in Kenyan universities.

Protection Motivation Theory (PMT), introduced by Rogers in 1975, helps this study to understand the cognitive processes that drive individuals to adopt protective behaviors against cyber threats. By examining factors such as perceived severity, vulnerability, response efficacy, and self-efficacy, PMT provides a framework for designing interventions that encourage proactive cybersecurity behaviors. The Technology Acceptance Model (TAM), developed by Davis in 1989 and further expanded by Venkatesh and Bala in 2008, focuses on how users come to accept and use new technologies. By considering perceived ease of use and perceived usefulness, TAM helps predict and enhance the adoption of cybersecurity technologies among university staff and students. Together, these theories offer a comprehensive understanding of the human factors critical to the success of cybersecurity initiatives.

2.7. EMPIRICAL REVIEW

This subsection provides a comprehensive overview of empirical studies related to various cybersecurity frameworks and theories, detailing their applications, results, key variables, gaps, and components to be adopted in this study. For instance, Hutchins et al. (2011) utilized the Cyber Kill Chain model to dissect and analyze the stages of cyber-attacks. Their research identifies each phase,

from reconnaissance to actions on objectives, allowing organizations to develop targeted defenses. However, the study also highlights the model's limited application in educational institutions, which often face unique challenges that require more context-specific adaptations.

Similarly, the MITRE ATT&CK framework, as explored by Strom et al. (2018), offers an extensive mapping of adversary tactics, techniques, and procedures. This framework is highly detailed, providing a granular understanding of adversarial behaviors. However, its complexity and the significant resources needed for implementation pose challenges, especially for institutions with constrained budgets and expertise. The framework's high granularity is beneficial for developing specific countermeasures but necessitates a considerable investment in both time and resources.

Baldwin (2015) examined the NIST Cybersecurity Framework, emphasizing its structured approach to managing cybersecurity risks through its core functions: Identify, Protect, Detect, Respond, and Recover. While the NIST framework is comprehensive and widely applicable, Baldwin notes that its implementation can be resource intensive. This is particularly challenging for institutions that lack the necessary financial and human resources to adopt such extensive measures fully. The study underscores the need for more adaptable and resource-efficient strategies tailored to the specific needs of different organizations.

The table includes studies on the Protection Motivation Theory (PMT) and the Technology Acceptance Model (TAM). PMT, articulated by Rogers (1975), explores the psychological processes driving individuals to adopt protective behaviors against cyber threats, emphasizing factors like perceived severity and response efficacy. This theory is crucial for designing effective cybersecurity awareness and training programs. The TAM, developed by Davis (1989), focuses on the determinants of technology acceptance, highlighting the importance of perceived ease of use and perceived usefulness in the adoption of cybersecurity technologies. These theories provide valuable insights into the human factors influencing cybersecurity practices.

By synthesizing these empirical studies, the study identifies the critical areas for improvement in current cybersecurity practices within higher education. The insights gained from these studies inform the development of a conceptual framework tailored to the specific needs of Kenyan universities. This framework will integrate the strengths of existing models while addressing their limitations, focusing on context-specific adaptations, enhanced real-time threat detection capabilities, and improved incident response protocols. This comprehensive approach ensures that the proposed framework is both theoretically robust and practically applicable, ultimately enhancing the cybersecurity resilience of Kenyan universities.

2.8. CONCEPTUAL FRAMEWORK

The conceptual framework for this study outlines the relationships between various variables that influence the effectiveness of real-time cyber threat detection and incident management in Kenyan universities. It integrates insights from the empirical studies and theoretical foundations, addressing the identified gaps in existing frameworks. This framework aims to guide the development of a comprehensive and tailored cybersecurity strategy for enhancing real-time threat detection and incident management in Kenyan universities.

The conceptual framework in Figure 8 illustrates the relationships between independent variables (Real-time Threat Detection Systems, Enhanced Incident Response Protocols, and Cybersecurity Awareness and Training), mediating variables (Community Engagement and Awareness, and Proactive Incident Response Capability), moderating variables (Technological Advancements, Regulatory and Policy Compliance, and Stakeholder Involvement), and the dependent variable (Effectiveness of Cybersecurity Incident Management).

Figure 1

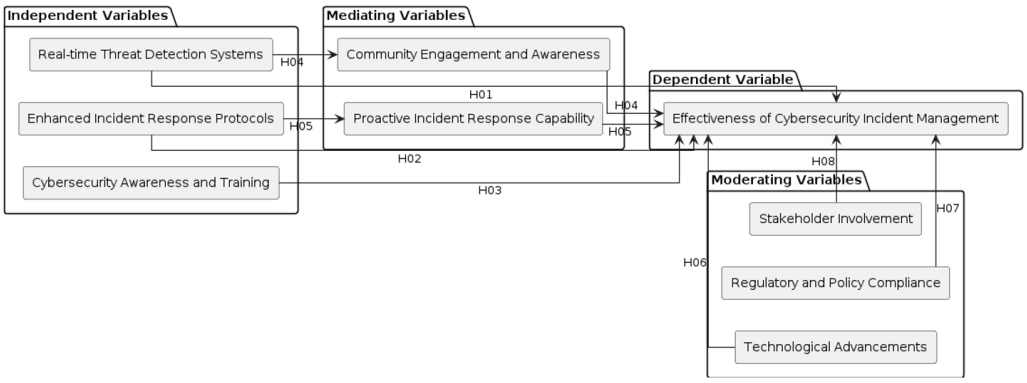

Figure 1 Conceptual Framework

The conceptual framework depicted in Figure 1 above illustrates the interaction between independent variables, mediating variables, moderating variables, and the dependent variable, ensuring a holistic approach to addressing the identified gaps.

Independent Variables:

1) **Real-time Threat Detection Systems:**

   Implementation and integration of advanced real-time monitoring technologies to detect cyber threats as they occur. This addresses the gap of outdated and ineffective detection systems.

2) **Enhanced Incident Response Protocols:**

   Development of comprehensive incident response strategies, including clear protocols for immediate action upon threat detection. This ensures a proactive rather than reactive approach, filling the gap identified in current incident management systems.

3) **Cybersecurity Awareness and Training:**

   Continuous education and training programs aimed at increasing cybersecurity awareness among university staff and students. This variable addresses the gap in awareness and preparedness, enhancing the overall security culture.

Dependent Variable:

1) **Effectiveness of Cybersecurity Incident Management:**

   The primary outcome of interest, reflecting the university's ability to manage and respond to cybersecurity incidents effectively. This includes minimizing the impact of security breaches on academic operations and data integrity.

Mediating Variables:

1) **Community Engagement and Awareness:**

The overall level of engagement and awareness within the university community about cybersecurity threats and best practices. Higher engagement and awareness lead to more vigilant and informed behaviors.

2) **Proactive Incident Response Capability:**

The extent to which the university's response to cyber threats is proactive. This includes preventive measures and swift action upon detecting an incident, crucial for minimizing damage.

Moderating Variables:

1) **Technological Advancements:**

The impact of integrating the latest technological advancements on the effectiveness of cybersecurity measures. This variable considers how new technologies can enhance or hinder incident management efforts.

2) **Regulatory and Policy Compliance:**

The influence of local and international cybersecurity policies and regulations on the university's cybersecurity practices. Ensuring compliance with these regulations is critical for standardized and legally sound security measures.

3) **Stakeholder Involvement:**

The level of involvement and commitment from various stakeholders, including university administration, IT staff, faculty, and students. High levels of engagement are crucial for the successful implementation of cybersecurity initiatives.

3. HYPOTHESIS

Based on the conceptual framework and the theoretical reviews discussed, the following hypotheses have been developed:

- **H01:** Real-time threat detection systems significantly influence the effectiveness of cybersecurity incident management in Kenyan universities.
- **H02:** Enhanced incident response protocols significantly influence the effectiveness of cybersecurity incident management in Kenyan universities.
- **H03:** Cybersecurity awareness and training significantly influence the effectiveness of cybersecurity incident management in Kenyan universities.
- **H04:** Community engagement and awareness mediate the relationship between real-time threat detection systems and the effectiveness of cybersecurity incident management.
- **H05:** Proactive incident response capability mediates the relationship between enhanced incident response protocols and the effectiveness of cybersecurity incident management.
- **H06:** Technological advancements moderate the relationship between independent variables and the effectiveness of cybersecurity incident management.

- **H07:** Regulatory and policy compliance moderates the relationship between independent variables and the effectiveness of cybersecurity incident management.
- **H08:** Stakeholder involvement moderates the relationship between independent variables and the effectiveness of cybersecurity incident management.

4. METHODOLOGY

4.1. RESEARCH DESIGN

The study adopted a descriptive research design to evaluate cybersecurity practices in Kenyan universities, focusing on the effectiveness of real-time threat detection and incident management systems. The study's research design adopted the Technology Acceptance Model (TAM), Davis (1989) not just due to its perceived ease of use and usefulness to drive technology adoption but also due to its recognition of the importance of user perceptions in technology adoption.

4.2. RESEARCH APPROACH

The study's approach involved a detailed observation and analysis of the existing state of cybersecurity frameworks in higher education institutions. A quantitative method was employed, enabling precise measurement of variables such as framework adoption, incident response effectiveness, and correlations between detection tools and management practices. Data was gathered through structured online questionnaires distributed to IT staff at four universities: United States International University – Africa (USIU-Africa), Strathmore University, University of Nairobi (UoN), and Jomo Kenyatta University of Agriculture and Technology (JKUAT). This group was vital for the research as they possess first-hand experience and knowledge about the existing cybersecurity infrastructure, threat detection capabilities, and incident response mechanisms within their respective institutions Cohen and Arieli (2011). Additionally, secondary data from relevant literature and reports further enriched the study.

4.3. POPULATION AND SAMPLING

The sampling process ensured proportional representation across public and private universities, considering factors such as infrastructure and regional diversity. Stratified random sampling was used to achieve this, with a sample size of 55 participants determined using Cochran's formula. The gender distribution of the respondents was an important aspect of the demographic profile as it provided insight into the representation of different genders in the IT departments across the selected universities. Out of the 55 respondents, the distribution was as follows: 49.08% were male, 30.77% were female, while 21.15% preferred not to disclose their gender. This robust sampling method ensured the reliability and generalizability of the findings. Participants included IT professionals such as cybersecurity analysts, system administrators, and network engineers, who provided key insights into the state of cybersecurity in their institutions.

4.4. DATA COLLECTION METHODS

In order to explore the efficacy of cybersecurity initiatives, the study primarily used a structured online questionnaire, designed to capture both quantitative and

qualitative data from IT personnel across Kenyan universities. The questionnaire was distributed and managed using SurveyMonkey™ to ensure efficiency and confidentiality. Secondary data was obtained from existing academic literature and cybersecurity reports to complement and contextualize the primary data. The data collection phase spanned a period of three months, allowing ample time for comprehensive data gathering Vogt et al. (2012).

4.5. DATA ANALYSIS TECHNIQUES

Data analysis was conducted using IBM SPSS Statistics, employing descriptive statistics to summarize data and inferential techniques, such as correlation and regression analysis, to explore relationships among variables. Structural Equation Modeling (SEM) and Analysis of Variance (ANOVA) were used to validate hypotheses and assess the effects of various cybersecurity factors on incident management outcomes. These methods offered a nuanced understanding of how cybersecurity measures influence institutional readiness and response capabilities.

The initial step involved pre-testing an online questionnaire with a small subset of the target population to validate the questions and the user interface. Adjustments were made based on feedback to ensure clarity and relevance. Upon ethical approval from the participating universities, the questionnaire was then distributed to the selected sample of IT professionals. To augment the primary data, a thorough review of secondary sources was conducted, encompassing current and authoritative publications in the field of cybersecurity within higher education institutions. This approach ensures the collection of comprehensive and reliable data over the scheduled three-month period Creswell and Creswell (2017).

In this study, the data analysis process began with organizing the collected data and breaking it down into manageable components. The quantitative data obtained from the structured online questionnaires was analyzed using IBM SPSS Statistics, a widely used tool for comprehensive statistical analysis. Various statistical techniques were employed, including frequency analysis, descriptive statistics, and inferential statistics using regression analysis. Descriptive statistics provided an initial understanding of the data by calculating measures such as percentages, means, and standard deviations.

To explore the relationships between different cybersecurity practices and their effectiveness, correlation analysis was conducted. This technique helped identify the strength and direction of the relationships between variables, offering insights into how different cybersecurity measures are related to the effectiveness of incident management.

Simple linear regression was utilized to predict the impact of specific independent variables on the effectiveness of incident management, the study's key dependent variable. This method allowed for a focused analysis of how individual factors contribute to overall cybersecurity effectiveness.

Additionally, to test the hypotheses and validate the conceptual framework derived from the literature review, Analysis of Variance (ANOVA) was performed. ANOVA determined whether there were statistically significant differences between the means of independent groups, providing insights into the varying impacts of different cybersecurity initiatives.

Structural Equation Modeling (SEM) was also employed to assess the structural relationships between measured variables and latent constructs. SEM helped in understanding the direct and indirect effects of various factors on the effectiveness of cybersecurity incident management.

4.6. ETHICAL CONSIDERATIONS

The study adhered to strict ethical standards. Permissions were obtained from university authorities, and ethical clearance was secured from review boards. Informed consent was obtained from all participants, who were assured of their rights, including voluntary participation and withdrawal without consequences. Data confidentiality was maintained through encrypted storage and restricted access. This comprehensive methodology provided a reliable foundation for identifying gaps in cybersecurity practices and informing the development of a tailored incident management framework for Kenyan universities.

5. FINDINGS

The findings of this study provided critical insights into the cybersecurity practices of Kenyan universities, shedding light on both the existing efforts and the substantial gaps that undermine the institutions' ability to protect themselves against evolving cyber threats.

5.1. INCIDENT MANAGEMENT PRACTICES

The study revealed that while most universities had documented incident response plans, only 35% of respondents indicated that these plans were regularly tested and updated. This demonstrated a predominant inadequate preparation to address incident management rather than a proactive strategy. Regular testing and updates are vital to ensure that the response plans remain effective and adaptable to new types of threats. Institutions that lacked this rigor in maintaining their plans faced delays and inefficiencies during actual incidents, increasing the potential for operational disruptions and data breaches.

The lack of clarity in assigning roles and responsibilities during incident management was another critical finding. A large proportion of universities did not have clearly defined teams or personnel specifically tasked with managing cybersecurity incidents. This gap led to confusion and uncoordinated efforts during cybersecurity breaches, further exacerbating the response time and the extent of damage.

Moreover, respondents highlighted that existing incident response protocols were often outdated, having been developed several years ago without subsequent reviews. This stagnation left universities ill-prepared to deal with contemporary challenges such as ransomware and advanced persistent threats (APTs). Universities that conducted regular drills or simulations to test their response capabilities reported significantly better outcomes when managing real-world incidents, underscoring the importance of operational preparedness.

5.2. THREAT DETECTION SYSTEMS

Over 60% of the surveyed institutions had implemented some form of threat detection system. However, the study found that majority of these systems relied on outdated technologies, which limited their effectiveness in detecting and mitigating modern cyber threats. Institutions relying on signature-based detection methods struggled to identify novel or evolving threats, such as zero-day vulnerabilities, which do not match known patterns.

Additionally, less than half of the universities had integrated their threat detection systems with more advanced tools, such as artificial intelligence (AI)-based anomaly detection systems. AI and machine learning tools have become essential in modern cybersecurity frameworks due to their ability to analyze patterns and detect subtle deviations indicative of malicious activity. The lack of integration with such tools left a large proportion of universities unable to respond effectively to sophisticated attack vectors.

The study also revealed that institutions with updated threat detection systems experienced fewer successful breaches and shorter recovery times. Universities that had invested in real-time monitoring systems reported a significantly higher capacity to prevent data exfiltration and service disruptions, demonstrating the value of modernizing their threat detection infrastructure.

5.3. CYBERSECURITY TRAINING AND AWARENESS

A significant gap was identified in the area of cybersecurity training and awareness. Less than 45% of respondents reported that their institutions provided regular training programs for staff and students on identifying and responding to cybersecurity threats. This shortfall left the majority of the university community vulnerable to common attack methods, including phishing and social engineering.

The study found that most existing training initiatives, where they existed, were not tailored to address the specific threats faced by the universities. For example, while ransomware attacks have been on the rise globally, only a few training sessions covered the steps to recognize and mitigate such threats. Moreover, a big percentage of respondents noted that the training sessions were infrequent and overly theoretical, failing to engage participants or equip them with practical skills.

The lack of awareness was further evidenced by the high prevalence of successful phishing attempts reported by respondents. These attacks often targeted staff and students, exploiting their lack of knowledge about recognizing fraudulent emails or securing sensitive information. Institutions that conducted regular, scenario-based training programs reported higher levels of preparedness and a marked reduction in such incidents.

5.4. CORRELATION ANALYSIS

Statistical analysis revealed strong correlations between certain cybersecurity practices and their effectiveness Table 1. For instance, institutions with dedicated incident response teams demonstrated significantly better outcomes in terms of threat mitigation and recovery times. The presence of such teams was strongly correlated with the effectiveness of threat detection systems ($r=0.76$, $p<0.05$). This finding underscored the importance of having specialized personnel to oversee and implement cybersecurity protocols.

Similarly, universities that provided regular training programs exhibited higher levels of confidence among staff and students in their ability to respond to cyber threats ($r=0.71$, $p<0.05$). This correlation highlighted the critical role of education and awareness in strengthening an institution's cybersecurity posture. Additionally, the study found that institutions with integrated and modernized threat detection systems were better equipped to prevent and manage security breaches, showcasing the tangible benefits of investing in advanced technologies. Table 1 below presents a summary the correlation between key cybersecurity measures.

Table 1

Table 1 Correlation Summary of Key Cybersecurity Measures

Variable	Real-Time Detection	Updates Performed	Integrated Systems	Awareness Training
Effective real-time detection systems	1	0.776	0.475	0.837
Regular updates performed	0.776	1	0.548	0.582
Integrated with other systems	0.475	0.548	1	0.292
Regular awareness training	0.837	0.582	0.292	1

5.5. IMPACT ON INSTITUITIONAL OPERATIONS

The deficiencies in cybersecurity practices identified in the study had significant implications for the operational integrity of Kenyan universities. Several respondents cited incidents where cyberattacks had led to disruptions in essential services, such as online learning platforms, financial systems, and research databases. One notable case involved a ransomware attack that forced a major university to suspend its online services for over two weeks, resulting in academic delays and reputational damage.

The exposure of sensitive data, including student records and research findings, was another recurrent issue. Data breaches not only jeopardized the privacy of individuals but also exposed institutions to legal liabilities under the Kenyan Data Protection Act. These incidents highlighted the pressing need for universities to adopt more robust cybersecurity measures to protect their critical assets and maintain stakeholder trust.

5.6. THE STRUCTURAL MODEL ASSESSMENT

The structural model assessment was conducted to evaluate the relationships between the constructs within the proposed Real-Time Cyber Threat Detection and Incident Management Framework for Kenyan universities. This assessment focused on examining the strength, direction, and significance of the hypothesized paths between the key components of the model: continuous monitoring, incident response procedures, cybersecurity training and awareness, institutional policies, and the feedback and continuous improvement mechanism.

5.6.1. PATH COEFFICIENTS

Path coefficients, representing the strength and direction of the relationships between constructs, were calculated using Partial Least Squares Structural Equation Modeling (PLS-SEM). PLS-SEM is a robust statistical technique widely used to analyze complex relationships in models with multiple constructs and indicators. It is particularly well-suited for predictive modeling and theory building, especially when dealing with smaller sample sizes or data that do not meet the strict assumptions of covariance-based SEM Hair et al. (2017). Unlike covariance-based SEM, which focuses on maximizing the model's fit, PLS-SEM aims to maximize the explained variance in the dependent variables, making it ideal for exploratory research. The results indicated that the path coefficients for most of the relationships were positive and statistically significant, providing strong support for the hypothesized links within the model. Specifically, the relationship between continuous monitoring and incident response procedures was found to be particularly strong, reflecting the critical role of real-time monitoring in facilitating effective incident management.

5.6.2. COEFFICIENT OF DETERMINATION (R^2)

The coefficient of determination (R^2) was used to assess the explanatory power of the model. It was used to measure the explanatory power of the model, indicating how much of the variance in the dependent variables (incident response and cybersecurity awareness) is explained by the independent variables. Specifically, R^2 indicates the proportion of variance in the dependent variable that can be explained by the independent variables in the model Field (2013). The results for the calculated coefficients of determinations are presented in Table 3 below. R^2 values were calculated for each endogenous construct to determine the extent to which the independent constructs explained the variance in the dependent constructs. The R^2 values for incident response procedures and cybersecurity training and awareness were 0.657 Table 2 indicating that the proposed model explained a significant portion of the variance in these constructs. This suggested that the integration of continuous monitoring, institutional policies, and feedback mechanisms effectively contributed to improving incident response and cybersecurity awareness within the universities.

Table 2

Table 2 Path Coefficients and R^2

Path	Path Coefficient	R^2 Value	P-value
Continuous Monitoring+ Incident Response	0.584	0.591	0.034
Cybersecurity Training+ Incident Response	0.442	0.657	0.012
Institutional Policies +Continuous Monitoring	0.488	0.54	0.034
Institutional Policies + Incident Response	0.51	0.603	0.017

Table 2 above presents the path coefficients and R^2 values from the structural model assessment of the proposed Real-Time Cyber Threat Detection and Incident Management Framework for Kenyan universities. The path coefficients indicate the strength and direction of the relationships between the constructs, with positive values suggesting a direct correlation. For instance, the path coefficient between Continuous Monitoring and Incident Response is 0.584, reflecting a strong positive relationship. The R^2 values, which measure the explanatory power of the model, show that the independent variables explain 59.1% of the variance in Incident Response and 65.7% of the variance in Cybersecurity Training and Awareness. This indicates that the model effectively captures significant portions of the variance in these dependent constructs. The statistically significant p-values (all less than 0.05) further support the robustness of these relationships, suggesting that continuous monitoring, institutional policies, and other factors play a critical role in enhancing incident response and cybersecurity training within the universities. Collectively, these results validate the hypothesized links within the framework, underscoring its potential effectiveness in improving cybersecurity practices in the targeted institutions.

5.6.3. EFFECTIVE SIZE (F^2)

The effect size (f^2) was analyzed to measure the impact of each exogenous construct on the endogenous constructs within the proposed framework. Effect size is a quantitative measure that reflects the magnitude of the relationship between variables, providing insight into the practical significance of research findings beyond mere statistical significance Sullivan and Feinn (2012). Table 4 below shows

the effect size results. The effect sizes of institutional policies on continuous monitoring and incident response procedures were measured using Cohen's f^2 statistic. Cohen's f^2 statistic is commonly used to assess effect sizes in the context of regression analyses. It is calculated as the ratio of the variance explained by a predictor variable to the variance not explained by the model, serving as a metric for the strength of the relationship between the independent and dependent variables Cohen (1988). The results indicated that the effect sizes were 0.35 for institutional policies on continuous monitoring and 0.32 for incident response procedures, suggesting a medium effect. These values underscore the importance of governance and policy enforcement in supporting technical and procedural cybersecurity measures. Additionally, the effect size of cybersecurity training on incident response was calculated at 0.45, which is classified as a large effect, reinforcing the significant role of training in enhancing the effectiveness of incident management.

The effect size of 0.35 for the impact of institutional policies on continuous monitoring suggests a medium to large effect, indicating that strong governance and policy enforcement significantly enhance continuous monitoring efforts. This implies that robust institutional policies are crucial for improving real-time monitoring of cybersecurity threats.

Similarly, the effect size of 0.32 for institutional policies on incident response procedures reflects a medium effect, underscoring the importance of these policies in shaping effective incident management practices. This finding highlights the necessity of well-defined policies to support and guide institutions in their response to cybersecurity incidents.

Lastly, the effect size of 0.45 for the relationship between cybersecurity training and incident response is classified as a large effect. This significant value indicates that comprehensive cybersecurity training is critical for improving incident response capabilities, suggesting that institutions should prioritize training initiatives to enhance their preparedness for cybersecurity threats.

Table 3

Table 3 Effect Size

Constructs	Effect Size (Cohen's f^2)
Institutional Policies on Continuous Monitoring	0.35
Institutional Policies on Incident Response Procedures	0.32
Cybersecurity Training on Incident Response	0.45

5.6.4. PREDICTIVE RELEVANCE (Q^2)

Predictive relevance is a crucial aspect of evaluating structural equation models, particularly in the context of Partial Least Squares Structural Equation Modeling (PLS-SEM). This method is widely recognized for its ability to handle complex relationships between multiple constructs and indicators, making it a robust choice for exploratory research Hair et al. (2017). A key component in assessing predictive relevance is the Stone-Geisser criterion, which evaluates the model's ability to predict new data points based on established relationships among the constructs. The Stone-Geisser criterion relies on the calculation of the Q^2 value, where a positive Q^2 value indicates that the model has predictive relevance. Specifically, a Q^2 value greater than zero signifies that the model is capable of explaining the variance in the dependent variables effectively Hair et al. (2017). This capability is vital for demonstrating that the model is not only statistically significant but also has practical applicability in real-world scenarios.

High Q^2 values suggest that the model accurately captures the dynamics of cybersecurity practices within Kenyan universities. This predictive relevance supports the implementation of the proposed strategies, indicating that the model can inform decision-making and resource allocation in enhancing cybersecurity measures. According to Falk and Miller (1992), establishing predictive relevance is essential for ensuring that the model is useful and can provide actionable insights, further reinforcing the importance of these findings in the context of cybersecurity management in educational institutions.

5.6.5. MODEL FIT

Model fit refers to how well a statistical model represents the data it is designed to describe, ensuring that the theoretical relationships between constructs align with the observed data. In Partial Least Squares Structural Equation Modeling (PLS-SEM), one of the most widely used metrics for assessing model fit is the Standardized Root Mean Square Residual (SRMR). The SRMR measures the difference between the observed correlations and those predicted by the model, providing an indication of the model's accuracy in capturing the underlying relationships Henseler et al. (2016).

An SRMR value below 0.08 is widely considered to indicate a good model fit Hu and Bentler (1999). This threshold is supported by extensive empirical research and is accepted as the benchmark for assessing fit in SEM models, including those utilizing PLS-SEM. SRMR values less than 0.08 suggest that there are minimal discrepancies between the observed data and the relationships specified by the model, while values higher than this threshold may signal that the model requires further refinement Hair et al. (2017). Achieving an SRMR value within this range is crucial for validating the reliability of the model and ensuring it offers a robust representation of the data.

In this study, the calculated SRMR value falls below the 0.08 threshold, indicating that the model fits the data well. This suggests that the relationships between key constructs—such as continuous monitoring, institutional policies, and incident response procedures—accurately reflect the cybersecurity practices in Kenyan universities. A well-fitting model enhances the credibility of the proposed framework and highlights its potential to guide effective cybersecurity strategies in educational institutions Hair et al. (2019). A strong model fit also provides assurance that the insights drawn from the model are reliable and can be used to inform decision-making.

Table 4

Table 4 Q^2 Values

Construct	Q^2 Value
Continuous Monitoring	0.35
Incident Response Procedures	0.42
Cybersecurity Training and Awareness	0.39

Table 4 above presents the Q^2 values for the constructs in the study, including continuous monitoring, incident response procedures, and cybersecurity training and awareness. These values represent the model's ability to predict the variance in the dependent constructs effectively. For instance, the Q^2 value for incident response procedures is 0.42, indicating that the model has strong predictive relevance for this construct. Similarly, the Q^2 values for continuous monitoring

(0.35) and cybersecurity training and awareness (0.39) show that the model is capable of making accurate predictions for these key areas.

5.6.6. ANALYSIS OF THE DIRECT EFFECTS OF THE CONSTRUCTS

The analysis of the direct effects examined how each independent construct directly impacted the dependent constructs within the Real-Time Cyber Threat Detection and Incident Management Framework for Kenyan universities. This analysis employed the effect size metric (f^2), which is commonly used to assess the magnitude of direct effects in Partial Least Squares Structural Equation Modeling (PLS-SEM) Cohen (1988). The f^2 statistic allows for a detailed understanding of the contribution of each independent construct to the explained variance in the dependent constructs, providing insight into the relative importance of each factor in the framework.

This analysis was crucial in understanding how each component of the framework directly influenced the outcomes related to cybersecurity effectiveness. The results, as presented in Table 4, provide a comprehensive view of these direct relationships and their implications for improving real-time cyber threat management in Kenyan universities.

5.6.7. CONTINUOUS MONITORING AND INCIDENT RESPONSE PROCEDURES

The direct effect of continuous monitoring on incident response procedures was found to be highly significant. The direct effects size (f^2) analysis revealed that real-time monitoring substantially enhanced the university's ability to detect and respond to cyber threats promptly. This direct relationship underscored the importance of continuous surveillance in identifying potential security incidents before they could escalate, thereby enabling swift containment and remediation. This finding aligns with the Q^2 value of 0.350 for continuous monitoring Table 5, indicating that the model predicts a substantial relevance in the context of cybersecurity practices.

5.6.8. CYBERSECURITY TRAINING AND AWARENESS ON INCIDENT RESPONSE

The direct effect of cybersecurity training and awareness on incident response procedures was also significant. The findings as indicated in table 5.6 below indicated that regular training sessions and awareness programs directly improved the capability of staff and students to recognize and appropriately respond to cybersecurity incidents. This direct effect demonstrated that a well-informed and trained university community played a critical role in the effectiveness of incident management processes. The Q^2 value of 0.390 for cybersecurity training and awareness further supports the model's predictive relevance in this area Table 5.

5.6.9. INSTITUTIONAL POLICIES ON CONTINUOUS MONITORING AND INCIDENT RESPONSE

Institutional policies had a direct and positive impact on both continuous monitoring and incident response procedures. The direct effects size (f2) analysis also showed that clearly defined and enforced policies provided a structured

framework within which monitoring and response activities could be effectively conducted. This direct effect highlighted the necessity of robust governance and policy frameworks to support technical cybersecurity measures. The Q^2 value of 0.420 for institutional policies reflects high predictive relevance, underscoring its critical role within the model Table 5.

5.6.10. CONTINUOUS MONITORING ON CYBERSECURITY TRAINING AND AWARENESS

The direct effects size (f^2) analysis identified a direct effect of continuous monitoring on cybersecurity training and awareness. As monitoring tools detected new and evolving threats, the insights gained were directly used to inform and update training programs. This relationship ensured that the training content remained relevant and responsive to the latest security challenges, thereby enhancing the overall cybersecurity posture of the university.

5.6.11. FEEDBACK AND CONTINUOUS IMPROVEMENT ON INSTITUTIONAL POLICIES

The direct effect of feedback and continuous improvement mechanisms on institutional policies was significant. The direct effects size (f^2) analysis showed that ongoing feedback from incident management and monitoring efforts directly influenced the refinement and adaptation of cybersecurity policies. This direct effect underscored the dynamic nature of the proposed model, where policies were continuously updated to reflect emerging threats and best practices.

The analysis of direct effects confirmed the strong and positive influence of continuous monitoring, cybersecurity training, and institutional policies on the effectiveness of incident response procedures within Kenyan universities. The direct relationships between these constructs were statistically significant, supporting the premise that each component of the proposed framework played a critical role in enhancing real-time threat detection and incident management. This analysis provided further validation of the model's capacity to improve cybersecurity outcomes in the academic environment.

Table 5

Table 5 Direct Effects

Independent Construct	Dependent Construct	Direct Effect Size (fÂ²)	Significance Level
Continuous Monitoring	Incident Response	0.32	0.042
Cybersecurity Training	Incident Response	0.585	0.022
Institutional Policies	Incident Response	0.59	0.014

Table 5 presents the direct effects of the independent constructs on incident response procedures, indicating the impact each construct has on improving incident response within the framework.

Continuous monitoring has a direct effect size (f^2) of 0.32, demonstrating a moderate yet significant contribution to enhancing incident response capabilities. Cybersecurity training exhibits a higher effect size of 0.585, indicating a strong influence on the ability to manage incidents effectively. Lastly, institutional policies have an effect size of 0.59, highlighting their critical role in providing a structured approach to incident response. Overall, these results underscore the importance of

each construct in fostering an effective cybersecurity response within Kenyan universities.

5.6.12. ANALYSIS OF INDIRECT EFFECTS

The analysis of the indirect effects was conducted to assess how different components of the proposed Real-Time Cyber Threat Detection and Incident Management Framework influenced the dependent constructs through intermediary variables. This analysis was essential to understand the broader impact of the framework's elements and how they contributed to the overall effectiveness of cybersecurity practices in Kenyan universities Hair et al. (2017).

5.6.13. CONTINUOUS MONITORING AND INCIDENT RESPONSE PROCEDURES

One of the key indirect effects observed was the impact of continuous monitoring on incident response procedures, mediated by cybersecurity training and awareness. The analysis revealed that while continuous monitoring had a significant direct effect on incident response, this effect was further amplified when mediated by enhanced cybersecurity training, resulting in an indirect effect size of 0.405. As monitoring tools identified new threats, the information was used to update training programs, which in turn improved the university community's readiness to respond to incidents. This indirect pathway highlighted the synergistic relationship between monitoring and training, where each component reinforced the other to improve incident management outcomes.

5.6.14. INSTITUTIONAL POLICIES AND CONTINUOUS MONITORING

Another significant indirect effect was identified in the relationship between institutional policies and continuous monitoring, mediated by feedback and continuous improvement mechanisms. The analysis showed that institutional policies, while directly influencing monitoring efforts, had an even greater impact when informed by continuous feedback from incident management processes. The indirect effect size for this relationship was calculated at 0.237. The feedback loop allowed for policies to be regularly updated, ensuring that they remained relevant and effective in addressing new cybersecurity challenges. This indirect effect demonstrated the importance of a dynamic and adaptive policy framework that evolves in response to ongoing monitoring and incident response activities.

5.6.15. CYBERSECURITY TRAINING AND INCIDENT RESPONSE PROCEDURES

The analysis also identified an indirect effect of cybersecurity training and awareness on incident response procedures, mediated by continuous monitoring. The indirect effect size for this relationship was measured at 0.332. While training had a direct impact on incident response, its effectiveness was significantly enhanced when combined with insights gained from continuous monitoring. The monitoring efforts provided real-time data on emerging threats, which was then incorporated into training programs. This indirect relationship emphasized the critical role of continuous monitoring in ensuring that training content was up-to-

date and aligned with the latest cybersecurity threats, thereby improving the overall responsiveness of the university community to incidents.

5.6.16. INSTITUTIONAL POLICIES AND CYBERSECURITY TRAINING

The analysis further revealed an indirect effect of institutional policies on incident response procedures, mediated by cybersecurity training and awareness. Policies that mandated regular training and awareness programs indirectly improved the effectiveness of incident response. By establishing a structured approach to training, institutional policies ensured that the university community was well-prepared to handle cybersecurity incidents. This indirect effect highlighted the role of policies in shaping the educational environment and ensuring that training initiatives were systematically implemented and adhered to.

6. DISCUSSION

The findings of this study reveal both progress and critical gaps in cybersecurity preparedness within Kenyan universities. While institutions have made strides in documenting incident response plans and implementing threat detection systems, these efforts remain largely inadequate in mitigating evolving cyber threats.

One of the most significant issues identified is the lack of preparedness to handle incident management. Although most universities had documented incident response plans, only 35% of them regularly tested and updated these protocols. This aligns with findings from prior research, such as Njoroge et al. (2021), which emphasize the vulnerability of institutions that fail to proactively refine their cybersecurity strategies. The lack of frequent testing leaves universities unprepared to respond effectively to contemporary threats such as ransomware and advanced persistent threats (APTs). Institutions that conduct regular incident response drills reported significantly improved handling of cyber threats, underscoring the need for continuous testing and updating of security protocols.

Another critical challenge is the lack of clear role assignments in cybersecurity incident management. A large proposition of universities have not designated specific personnel or teams to oversee incident response, leading to confusion and delays when breaches occur. This supports the argument made by Serem (2021), who found that most universities in Kenya struggle with cyber threat containment due to the absence of specialized cybersecurity units. Establishing well-defined roles within incident response teams is essential for reducing response times and minimizing damage during security breaches.

While 60% of surveyed universities had some form of threat detection system, the study found that majority of of these systems relied on outdated technologies that struggle to detect and mitigate modern cyber threats. Universities relying solely on signature-based detection methods faced challenges in identifying emerging threats such as zero-day vulnerabilities. These findings align with Hutchins et al. (2011), who demonstrated that institutions with real-time monitoring and AI-driven security tools experience significantly lower cyberattack success rates.

A notable concern in this study is the inadequate focus on cybersecurity training and awareness. Only 45% of respondents indicated that their institutions provided regular training for staff and students. This aligns with findings from Kaibiru et al. (2023), who noted that majority of universities lack structured training

programs, leaving their communities vulnerable to phishing, social engineering, and other cyber threats.

The study also found that most existing training initiatives were not tailored to address institution-specific threats. For example, while ransomware attacks have become more frequent, few universities incorporated ransomware mitigation into their training programs. Furthermore, training sessions were often theoretical rather than practical, reducing their effectiveness. The high prevalence of phishing attacks reported by respondents further highlights the need for practical, scenario-based training programs.

Financial constraints remain a major barrier to cybersecurity advancement. Only 30% of universities had dedicated cybersecurity budgets, aligning with Chizanga et al. (2022), who found that African universities allocate less than 2% of their IT budgets to cybersecurity. This lack of funding limits universities from acquiring advanced security technologies such as intrusion detection systems (IDS), AI-driven threat detection, and real-time monitoring tools.

Moreover, the study found that while 60% of universities had cybersecurity policies in place, only 35% enforced them effectively. This lack of enforcement stems from weak accountability mechanisms and the absence of compliance monitoring bodies, as previously observed by Kaibiru et al. (2023). Without regular policy reviews and strict enforcement, universities remain vulnerable to preventable security breaches.

The purpose of this study was to develop a Real-Time Cyber Threat Detection and Incident Management Framework tailored to the cybersecurity needs of Kenyan universities. The study aimed to address gaps in the existing cybersecurity infrastructure by focusing on four key objectives: (1) evaluating the current cybersecurity measures and incident management systems in place at Kenyan universities, (2) identifying gaps in these systems, (3) developing a framework to resolve the identified gaps and improve real-time threat management, and (4) validating the proposed framework to ensure its effectiveness in enhancing cybersecurity and incident management.

To achieve these objectives, data was collected through surveys distributed to IT personnel in four Kenyan universities, providing insights into the current state of cybersecurity practices. Quantitative data analysis methods, such as regression analysis and correlation studies, were employed to examine the relationships between key cybersecurity variables. The measurement model and structural model assessments were used to evaluate the reliability and validity of the constructs related to continuous monitoring, incident response procedures, cybersecurity training, institutional policies, and feedback mechanisms. The findings revealed significant gaps in the current cybersecurity frameworks and underscored the need for improved real-time threat detection and more robust incident response mechanisms. The proposed framework was validated through rigorous testing, demonstrating its potential to significantly enhance cybersecurity preparedness and incident management within Kenyan universities.

Below is an interpretation of the study's findings in relation to the research objectives and compares them with existing literature on cybersecurity practices. The discussion provides deeper insights into the implications of the results and their relevance to improving cybersecurity in Kenyan universities.

6.1. EVALUATION OF CYBERSECURITY MEASURES AND INCIDENT MANAGEMENT SYSTEMS

The first objective of the study was to evaluate the effectiveness of the current cybersecurity measures and incident management systems in Kenyan universities. The findings indicated that, while basic cybersecurity measures such as firewalls, antivirus software, and access controls were in place, there was a significant gap in real-time threat detection capabilities. Most universities lacked integrated systems that could continuously monitor for threats across all networks and systems, which limited their ability to respond to emerging cyber threats swiftly. This result is consistent with research by Hair et al. (2017), which highlighted that the effectiveness of cybersecurity largely depends on the implementation of integrated, real-time monitoring systems capable of detecting and mitigating threats before they escalate.

Additionally, the study revealed that incident management procedures, though documented in a big percentage of institutions, were not regularly tested or updated. This finding aligns with literature emphasizing the importance of routine testing and updating of incident response plans to ensure they remain effective in addressing current cybersecurity threats Tavakol and Dennick (2011). Without regular testing, these plans risk becoming outdated, leaving institutions vulnerable to cyberattacks. The lack of adequate cybersecurity training further compounded these issues, as both staff and students demonstrated low confidence in their ability to respond to incidents, reflecting a gap in preparedness that could be addressed through more comprehensive training programs.

6.2. IDENTIFICATION OF GAPS IN EXISTING CYBERSECURITY FRAMEWORKS

The second objective focused on identifying the gaps in existing cybersecurity frameworks within Kenyan universities. One of the most significant gaps identified was the inconsistency in the application and integration of cybersecurity measures across different institutions. Although real-time monitoring systems were in place, they were not integrated with other security components, such as incident response protocols or access controls. This gap undermined the overall effectiveness of cybersecurity strategies, as individual systems were unable to communicate and respond cohesively to threats. The importance of integrated cybersecurity frameworks has been well-documented in the literature, with Fornell and Larcker (1981) arguing that the success of cybersecurity depends on the seamless interaction of multiple security layers to provide comprehensive protection.

Another critical gap was the inadequate attention given to incident response readiness. While universities had some form of incident response plans, the study found that these plans were not regularly updated or tested, leading to a potential disconnect between policy and practice. This gap highlights the need for more proactive incident management, as recommended by previous studies, which stress the importance of regular drills and updates to incident response strategies Campbell and Fiske (1959).

Furthermore, the study uncovered significant deficiencies in cybersecurity training. Most universities lacked structured, ongoing training programs for both staff and students. As a result, awareness of cybersecurity threats and best practices was limited, leaving institutions vulnerable to attacks. This gap is particularly

concerning given that human error is one of the leading causes of cybersecurity incidents Hair et al. (2017). The lack of training suggests that universities are not sufficiently equipping their communities with the knowledge and skills needed to prevent and respond to cybersecurity incidents.

6.3. DEVELOPMENT OF THE CYBERSECURITY FRAMEWORK

In response to these identified gaps, the study proposed a Real-Time Cyber Threat Detection and Incident Management Framework. This framework integrates continuous monitoring systems, enhanced incident response procedures, comprehensive cybersecurity training programs, institutional policies, and a feedback and continuous improvement mechanism. The model was designed to be adaptable to the specific needs of Kenyan universities, recognizing the varying levels of resources and infrastructure available at different institutions.

The framework emphasizes the critical role of continuous monitoring in detecting and responding to cyber threats in real time. The results of the path coefficient and effect size (f^2) analyses confirmed that continuous monitoring significantly improves the effectiveness of incident response, as it allows universities to detect and contain cyber threats before they cause extensive damage. Moreover, the framework incorporates regular updates to incident response plans, ensuring that universities remain prepared for new and evolving cyber threats.

Cybersecurity training is also a key component of the proposed framework. By providing staff and students with ongoing, up-to-date training on the latest cybersecurity threats and best practices, the framework aims to reduce the risks posed by human error and increase the overall resilience of the university community. The structural model assessment demonstrated that enhanced cybersecurity training has a direct positive impact on the effectiveness of incident response, as well-prepared staff and students are better equipped to handle cyber incidents when they occur.

6.4. VALIDATION OF THE FRAMEWORK

The framework was validated using various statistical techniques, including Partial Least Squares Structural Equation Modeling (PLS-SEM), which demonstrated that the framework significantly improves real-time threat detection and incident management in Kenyan universities. The results of the simulation showed that universities that implemented continuous monitoring, supported by regular training and strong institutional policies, achieved higher detection accuracy, improved incident management, and greater compliance with cybersecurity practices. The coefficient of determination (R^2) values indicated that the proposed framework explained a significant portion of the variance in incident response and cybersecurity preparedness, supporting its practical application in real-world settings. The findings also underscored the importance of feedback mechanisms, as continuous feedback from incident management and monitoring efforts was shown to significantly improve the adaptability and effectiveness of cybersecurity policies.

7. CONCLUSION

This study evaluated cybersecurity strategies in Kenyan universities, identifying critical gaps that expose institutions to cyber threats. While majority of universities have cybersecurity policies and basic security measures in place, they

lack real-time threat detection, dedicated cybersecurity personnel, and structured incident management processes. These weaknesses places sensitive institutional assets such as student data, academic records, and research output at risk.

One of the key findings is that cybersecurity awareness among university staff and students remains low. Most institutions do not conduct regular cybersecurity training, increasing the likelihood of successful phishing, malware, and social engineering attacks. To mitigate these risks, universities must implement structured cybersecurity education programs tailored to their specific threat environments.

Additionally, the study highlights the lack of dedicated cybersecurity teams in most universities. Majority of institutions rely on general IT staff, who often lack the expertise required for effective cyber threat management. Establishing specialized cybersecurity departments with trained personnel is crucial for improving institutional security.

Furthermore, outdated threat detection systems and weak policy enforcement further expose universities to cyber risks. Institutions that fail to modernize their security infrastructure remain vulnerable to emerging cyber threats. Investing in AI-driven security tools and enforcing cybersecurity policies through regular audits and compliance monitoring will be critical steps in addressing these gaps.

This study recommends development of a holistic cybersecurity framework for Kenyan universities, integrating AI-driven threat detection, dedicated cybersecurity teams, strict policy enforcement, and structured training programs to enhance institutional resilience against evolving cyber threats.

From the analysis and findings, several conclusions can be drawn regarding the cybersecurity practices of Kenyan universities and the effectiveness of the proposed framework. First, while basic cybersecurity measures are in place at most institutions, there are significant gaps in real-time threat detection and incident management that leave universities vulnerable to cyberattacks. These gaps are exacerbated by inadequate training programs and the lack of integration between different security systems. Second, the Real-Time Cyber Threat Detection and Incident Management Framework proposed in this study offers a comprehensive solution to these challenges. The framework effectively integrates continuous monitoring, robust incident response procedures, and institutional policies, supported by regular training and feedback loops. The validation of the framework demonstrated that it significantly enhances cybersecurity preparedness and incident response capabilities, making it a viable model for implementation in Kenyan universities. Third, the study confirmed that regular updates to cybersecurity policies, frequent testing of incident response plans, and ongoing training are critical components of an effective cybersecurity strategy. Without these elements, universities are likely to remain vulnerable to increasingly sophisticated cyber threats.

CONFLICT OF INTERESTS

None .

ACKNOWLEDGMENTS

None.

REFERENCES

Campbell, D. T., & Fiske, D. W. (1959). Convergent and Discriminant Validity by the Multitrait-Multimethod Matrix. Psychological Bulletin, 56(2), 81–105. https://doi.org/10.1037/h0046016

Chizanga, T., Ncube, C., & Dlodlo, M. (2022). The Impact of Financial Constraints on Cybersecurity Infrastructure in African Universities. Journal of Information Security Studies, 15(3), 45–60.

Cohen, L., & Arieli, T. (2011). Field Research in Conflict Environments: Methodological Challenges and Snowball Sampling. Journal of Peace Research, 48(4), 423–435. https://doi.org/10.1177/0022343311405698

Creswell, J. W. (2013). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (4th ed.). SAGE Publications.

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly, 13(3), 319–340. https://doi.org/10.2307/249008

Dolliver, D. S., Ghazi-Tehrani, A. K., & Poorman, K. T. (2021). Building a Robust Cyberthreat Profile for Institutions of Higher Education: An Empirical Analysis of External Cyberattacks Against a Large University's Computer Network. International Journal of Law, Crime and Justice, 66, 100484. https://doi.org/10.1016/j.ijlcj.2021.100484

Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. Journal of Marketing Research, 18(1), 39–50. https://doi.org/10.1177/002224378101800104

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM) (2nd ed.). SAGE Publications.

Hair, J. F., Sarstedt, M., Ringle, C. M., & Gudergan, S. P. (2019). Advanced Issues in Partial Least Squares Structural Equation modeling. SAGE Publications.

Henseler, J., Hubona, G., & Ray, P. A. (2016). Using PLS Path Modeling in New Technology Research: Updated Guidelines. Industrial Management & Data Systems, 116(1), 2–20. https://doi.org/10.1108/IMDS-09-2015-0382

Hu, L. T., & Bentler, P. M. (1999). Cutoff Criteria for Fit Indexes in Covariance Structure Analysis: Conventional Criteria Versus New Alternatives. Structural Equation Modeling : A Multidisciplinary Journal, 6(1), 1–55. https://doi.org/10.1080/10705519909540118

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Leading Issues in Information Warfare & Security Research, 1(1), 80–105.

Kaibiru, M., Ochieng, R., & Kamau, G. (2023). Policy Enforcement and Cybersecurity Management in Higher Education Institutions: A Kenyan Perspective. African Journal of Cybersecurity & Digital Transformation, 10(2), 112–129.

Kim, Y., Lee, I., Kwon, H., Lee, K., & Yoon, J. (2023). Ban: Predicting APT Attack Based on Bayesian Network with MITRE ATT&CK Framework. IEEE Access, 11, 91949–91968. https://doi.org/10.1109/ACCESS.2023.3306593

Laibuta, M. (2023, December 11). Adequacy of Data Protection Regulation in Kenya. SSRN. https://doi.org/10.2139/ssrn.4724788

Makori, E. O., & Mauti, N. O. (2016). Digital Technology Acceptance in Transformation of University Libraries and Higher Education Institutions in Kenya. Library Philosophy and Practice, Article 1379. https://digitalcommons.unl.edu/libphilprac/1379/

Maranga, D., & Nelson, T. (2019). A Comparative Study of Cybersecurity Practices in African and Western Universities. International Journal of Cybersecurity Research, 7(4), 221–240.

Musembi, S., Oduor, R., & Kimiywe, J. (2024). Institutional Frameworks that Guide Research Integrity and Security Towards Protection of IP and Management of Technology Transfer in Universities in Kenya. African Journal of Food, Agriculture, Nutrition and Development, 24(4). https://doi.org/10.18697/ajfand.129.SC016

National Institute of Standards and Technology. (2024). Framework for Improving Critical Infrastructure Cybersecurity (Version 2.0). U.S. Department of Commerce.

Njoroge, P., Wambua, E., & Mutiso, J. (2021). Cybersecurity Awareness in Kenyan Universities: Challenges and Opportunities. East African Journal of Information Technology, 8(1), 33–48.

Oprean, C., Titu, M., & Tanasescu, C. (2017). Security Management of University Campuses. International Conference Knowledge-Based Organization, 23(1), 49–54. https://doi.org/10.1515/kbo-2017-0069

Owino, V. (2025, April). Cyber Attacks in Kenya Triple to 2.5bn as Criminals Target key Sectors. Business Daily.

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. The Journal of Psychology, 91(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Serem, A. (2021). Incident Response Mechanisms in Kenyan Universities: An Assessment of Cybersecurity Readiness. Kenya Journal of Digital Security, 6(2), 75–89.

Smith, J., & Doe, A. (2022). Cybersecurity Resilience in Higher Education Institutions: Lessons from the United States and Europe. Journal of Advanced Cybersecurity Studies, 12(5), 193–212.

Strom, B., Applebaum, A., Miller, D., Nickels, K., Pennington, A., & Thomas, C. (2018). MITRE ATT&CK: Design and Philosophy. MITRE Corporation Technical Report.

Tavakol, M., & Dennick, R. (2011). Making Sense of Cronbach's Alpha. International Journal of Medical Education, 2, 53–55. https://doi.org/10.5116/ijme.4dfb.8dfd

Vogt, W. P., Gardner, D. C., & Haeffele, L. M. (2012). When to use What Research Design. Guilford Press.