Kabarak Journal of Research & Innovation

https://journals.kabarak.ac.ke/index.php/kjri/

RESEARCH ARTICLE

AN EMPIRICAL ASSESSMENT OF CYBERSECURITY MATURITY IN HIGHER LEARNING INSTITUTIONS

Beatrice A. Owino, Collins Oduor & Gerald Chege

Department of Computing & Informatics, School of Science & Technology,
United States International University Africa

Correspondence email: beatricej2009@gmail.com

Submitted: 7th August 2025; Accepted: 26th August 2025; Published (online): 3rd September 2025

ABSTRACT

Universities increasingly rely on digital infrastructure for academic, administrative, and research functions, making them prime targets for cyber threats. In developing regions, these risks are exacerbated by limited resources and weak enforcement of cybersecurity policies. This study assessed the cybersecurity maturity of universities within Nairobi County, focusing on Governance, technical capacity, and human factors. A descriptive research design was employed, using online questionnaires administered to IT personnel across 25 universities. Data was analyzed using SPSS, applying descriptive statistics to measure maturity across institutional domains.

Findings revealed that while most institutions had implemented basic technical controls such as antivirus software and firewalls, only 32% had formal cybersecurity policies. Human factors emerged as the most significant weakness, with low staff awareness, limited training, and inadequate incident response preparedness. Overall, institutions displayed moderate cybersecurity maturity, with clear strategic planning and governance structure gaps.

The study contributes to the limited empirical research on cybersecurity in higher learning institutions by offering data-driven insights into institutional preparedness. It provides a practical foundation for targeted interventions and capacity building. The study recommends the adoption of international frameworks, continuous staff training, and collaboration with national cybersecurity agencies to improve institutional resilience and cyber-readiness.

Keywords: Cybersecurity Maturity, Higher Learning Institutions, Risk Management, Cyber resilience, Network security, Vulnerability

INTRODUCTION

The rate of technological progress in computing has accelerated in the recent century. A complex integration of information systems (IS) and information and communication technology (ICT) is now an inevitable result of this progress, coupled with the pervasive globalization of businesses and organizations (Hina, Selvam, and Lowry, 2019). Modern companies and institutions prioritize cybersecurity risk assessment in response to the daily volume of data and an increase in successful cyberattacks. Information is a significant business asset in all organizations. According to

Karbowski and Jaskola (2023), the security of network and information systems may be defined as the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity, or confidentiality of stored, transmitted or processed data or the related services offered by, or accessible via, those network and information systems. The ICT systems are prone to failures caused by malicious actors attacking the systems, accidents, or even natural disasters that could interrupt their normal functions. These failures and interruptions are called cyber incidents, costing companies millions of euros every year (Sharma, 2022).

Kioskli and Polemi (2020) define cybersecurity threats as the potential cause of an unwanted incident that may harm a system or organization. It is the likelihood that a threat agent will exploit a vulnerability, negatively impacting the confidentiality, integrity, or availability of information. The unprecedented growth of network-connected devices has led to a noticeable increase in the activity of cyber attackers; thus, nowadays, any organization, including HLI, is concerned about cybersecurity aspects and their management. Accidental leakage of sensitive information in various organizations, including HLIs, has caused financial and reputational losses (Hina et al, 2019). Unfortunately, the number and severity of cybersecurity breaches in HLIs continually increase due to low cybersecurity awareness levels, employee negligence, lost or stolen devices, social media, malicious website attacks, Accidental disclosure of sensitive information, viruses/malware, and insecure third-party e-mail attachments (Hina et al, 2019). According to Marican, Razak, and Selamat (2023), poorly executed security measures result in poor cybersecurity, reflecting a low maturity level.

The primary objective of cybersecurity is to safeguard digital assets, including data, networks, and information systems, from unauthorized access, manipulation, or destruction. This encompasses protecting against various cyber threats and attacks, such as hacking, malware, phishing, Ransomware, and social engineering attacks (Alhumud, Omar, and Altohami, 2023). The study of Tsen, Ko, and Slapnicar (2022) indicates that organizations that suffered cyber-attacks had the following cyber resilience characteristics: a relatively low level of cyber resilience reflected in the low frequency of cybersecurity roles, low reliance on cybersecurity frameworks, and relatively low strength of prevention, detection, and recovery controls (Tsen et al, 2022). This study contributes to existing literature by providing empirical evidence on the cybersecurity maturity of HLIs in Nairobi County, an under-researched context in Sub-Saharan Africa. It identifies critical gaps in technical, institutional, and human domains, and offers practical recommendations aligned with international standards. The findings are a foundation for policymakers, institutional leaders, and cybersecurity professionals to develop targeted strategies for enhancing resilience in higher learning environments.

Objective of the paper

This paper aims to assess the cybersecurity maturity of universities within Nairobi County by examining existing governance structures, technical capabilities, and human factors to identify key gaps and recommend strategies for enhancing institutional cybersecurity resilience.

RELATED WORK

Challenges in Cybersecurity Risk Assessment in Higher Learning Institutions

Academic literature describes many challenges when it comes to cybersecurity risk assessments. These challenges can be attributed to various factors, ranging from economic constraints to infrastructural and Governance challenges (Kepuska and Tomasevic, 2024). Due to the open and collaborative environments of HLIs, cybersecurity risk assessment is critical for identifying, analyzing, prioritizing, and mitigating potential risks to an organization's digital assets and information systems.

Like other contemporary organizations, universities are growing their digital footprint, increasing their exposure to security breaches and necessitating ongoing work in security and privacy (Aborujilah et al, 2022). According to Ulven and Wangen (2021), identifying assets, threats, vulnerabilities, and events can be challenging as information assets are continuously created, processed, and stored. Among the most significant cybersecurity challenges facing the education sector is an increased number of cyberattacks that aim to steal personal information, extort data for money, or disrupt schools' ability to operate. Research shows that HLI has been regularly targeted and facing several challenges, including the following:

Governance Challenges

There is a lack of national cybersecurity policy strategies for HLI (Kepuska & Tomasevic, 2024). Many universities lack structured governance frameworks to guide risk assessment processes. Cybersecurity is often managed reactively, with little institutional emphasis on proactive risk identification. Leadership tends to perceive cybersecurity as a purely technical responsibility rather than a governance issue, leading to inadequate resource allocation and lack of accountability. Furthermore, universities rarely align their risk assessment activities with international frameworks such as ISO/IEC 27005 or NIST SP 800-30, which provide systematic methodologies. The lack of a comprehensive legal framework for cybersecurity in many African countries also poses a challenge (Nkambule and Jansen, 2024).

Human Factors

Effective risk assessment requires skilled personnel who can identify, analyze, and prioritize cyber risks. However, universities often suffer from a shortage of cybersecurity experts, and IT staff may not be adequately trained in structured risk assessment methodologies. Additionally, there is low awareness among academic and administrative staff, which limits the identification of risks arising from user behavior, such as phishing susceptibility or poor data handling practices. Resistance to change further hampers the institutional adoption of standardized assessment processes.

Technical Capacity Gaps

Risk assessment is data-driven, but many universities lack the necessary technical tools and infrastructure to collect, monitor, and analyze relevant security data. Outdated systems, weak logging mechanisms, and lack of automated monitoring make it difficult to detect vulnerabilities or measure risks accurately. Financial constraints also prevent investment in specialized risk management tools, forcing institutions to rely on ad hoc or manual assessments that are

inconsistent and incomplete. The HLI has limited budgets for cybersecurity (Fouad, 2021). It is estimated that spending on information security in the U.S. higher education sector is around 3.6 per cent of the institutions' IT budget, unlike in other sectors, like financial services, which spend around 10.9 per cent of their IT budgets on cybersecurity (Fouad, 2021). This situation does not improve when universities receive funding for new research projects, as rarely does part of this funding get allocated to IT security budgets, even though research data adds new targets that IT management needs to secure.

Evolving Cyber Threat Environment is also a challenge. Cyberspace's threat environment is continually changing, and new methods and tools make it hard to identify, evaluate, and map harmful attacks on an organization (Ulven and Wangen, 2021). Ganesen et al (2022) cited inadequate security measures and workforce preparation initiatives that have not been implemented within the HLI.

Regulatory and Policy Barriers

While Kenya's Data Protection Act (2019) and National ICT Policy (2020) provide a regulatory basis for improving cybersecurity, enforcement and compliance in the higher education sector remain weak. HLI often struggle to interpret and operationalize these requirements within their institutional contexts. Moreover, there is no sector-wide framework or shared platform for conducting or standardizing risk assessments across universities, resulting in fragmented and uneven practices.

Cybersecurity risk assessment in HLIs is constrained by weak governance structures, shortage of skilled staff, lack of technical tools, and limited enforcement of regulatory frameworks. These challenges reduce the effectiveness of risk assessment and prevent universities from achieving higher levels of cybersecurity maturity. Addressing them requires both institutional reforms and collaborative approaches, such as shared incident response hubs or sector-wide risk assessment frameworks, tailored to the realities of resource-constrained HLI.

Cyber Attack Types in Higher Learning Institutions

Cyber Security threats are any digital activity that could threaten content integrity or endanger access to data and users' privacy (Yousif Yaseen, 2022). Cyber threats to HLI IS and data come from various common attack vectors, including deliberate threats (e.g., ransomware attacks) and accidental acts (e.g., unintentional disclosure by an employee).

HLIs are rich in population and private data that attract substantial attacks. Yusif & Hafeez-baig, (2023) describe universities as "loosely coupled systems", thus open, making them susceptible to all sorts of physical attacks, necessitating a sense of balance between openness and safety. HLI's house not only has large and critical biographical data and financial data but also data on cutting-edge research and development of emerging and new technologies (Yusif & Hafeez-baig, 2023). Cyber-attacks against universities have been increasing in recent years, with the average cost of addressing a cyber-attack amounting to £620,000 in 2021 (Lallie and Titis, 2023). These attacks target sensitive data, intellectual property, financial information, and the overall integrity of academic and research activities. Cybersecurity threats and incidents negatively impact the

infrastructure and digital assets associated with HLIs and individuals and their reputations (Yaseen, 2022).

The types of attacks and threats on the security of information systems also vary, both from within the institution and from outside (Mantra et al., 2020). Cyberattacks on higher learning institutions can take various forms, each with unique characteristics and impacts. The attacks include Phishing Attacks, Ransomware Attacks, Distributed Denial of Service (DDoS) Attacks, Malware Attacks, and Insider Attacks.

Internal Threats

Internal threat is a critical security problem. Intimidation of intrinsic persons may be presented inadvertently or intentionally by injured persons. Internal threats are defined as threats posed by a person who has authorized access privileges and knowledge of an organization's computer systems and is inspired to affect the organization adversely. Lallie and Titis (2023) pointed out that having a unique level of institutional access, students may present a particular type of threat either as targets of phishing attacks or for deliberate malicious reasons such as viewing and altering grades, playing pranks, testing their hacking abilities, or carrying revenge.

Ndeda et al., (2019) noted that insider threats are characterized by employees deliberately attacking organizational cyberspace assets. High-level access users, for example, system administrators, look for system loopholes to gain unauthorized access, ride on other users' access privileges without their authority to attack the organizational systems for several reasons ranging from disgruntlement, revenge, and blackmail (Ndeda et al., 2019).

The literature discusses incidents of student grade manipulation, such as attacks at Austin's Business School and incidents in Kenyan colleges where some students' outstanding fees were changed (Maranga, 2019). Moreover, a student compromised over 3,300 accounts at the University of Alberta, whereas an insider at Rutgers University took down the institution's central authentication server that maintained the gateway portal to deliver assignments and assessments (Lallie and Titis, 2023).

Phishing Attacks

Al and Stefano (2022) define phishing as a typology of cyber-attacks heavily grounded in social engineering, where an attacker sends a malicious message to trick the victim into performing a specific action. Phishing is a problem that affects colleges and institutions frequently. Phishing attacks are performed by sending forged e-mails from an authentic entity looking legitimate to a victim or a group of victims (Salahdine et al., 2021). In a phishing attack, the hacker will assume the identity of a reliable source and take advantage of that relationship to coerce the user into disclosing personal data like passwords or even social security numbers (Pillay and Sharma, 2022) . Social engineering attacks can cost organizations more than 100,000 USD per instance (Alsulami et al., 2021). Phishing exploits the victim's lack of knowledge about technology or inattention to presented information.

Distributed Denial of Service (DDoS)

In a DDoS attack, the attacker floods a server or network with traffic or requests, overwhelming its capacity to respond to legitimate requests and causing it to crash or become unavailable to users (Haque et al, 2023). When an institution suffers a complete network outage from a Denial of Service (DoS) attack disrupting teaching and learning, it endures a dent in its status.

DDoS attacks can disrupt a university's online systems and services, including e-mail, websites, and learning management systems, causing significant disruption to students, staff, and faculty. In a DDoS attack, the attackers take control of a vast network of compromised computers or other devices and launch a concerted assault on the targeted system (Pillay & Sharma, 2022). According to Lallie & Titis (2023), 63 UK universities suffered from DDoS attacks in 2016, while in 2019, DDoS attacks continued to be on the rise, with a successful attack on the University of Edinburgh making headline news. In 2021, there was a 102% increase in such attacks targeting universities, colleges, and schools, with a DDoS attack occurring every three seconds (Lallie & Titis, 2023).

Ransomware

Ransomware, a subset of malware, is considered one of the most significant and rapidly expanding cyber threats to the digital world, and it is presently thought to be both the biggest threat to Internet users and the main source of cash for hackers. Yusif & Hafeez-baig (2023) define Ransomware as malicious software that, once loaded on a victim system, encrypts the hard drive and issues a warning that unless a ransom is paid within 24–48 hours, all the data will become unrecoverable. Hackers use Ransomware to target colleges and universities because they retain valuable student data and conduct important high-level research (Pillay and Sharma, 2022). According to Kepuska and Tomasevic (2024), HLIs are increasingly facing ransomware attacks, with a report indicating that nearly two-thirds (64%) of institutions experienced such attacks last year. Kepuska and Tomasevic (2024) cited that Ransomware attacks in HLIs have increased seven times in 2020 compared to 2019. Ransomware directly impacts educational institutions by encrypting critical files and restricting access for staff and students. Infections can encrypt files within three seconds, highlighting the urgency for protective measures (Mashila et al, 2025).

Studies show that the most significant rise in cyber-attacks has come from ransomware attacks. Ransomware attacks first occurred in 1989 in the healthcare domain, and it was estimated that WannaCry infected an estimated 10,000 organizations with 200,000 computers in more than 150 countries via phishing e-mails and a user visiting a malware-infected website (Yusif and Hafeez-Baig, 2023).

Although law enforcement does not encourage, endorse, nor condone the payment of ransom demands, several universities have reported paying cybercriminals to unlock their systems, such as Maastricht University in the Netherlands, paid nearly €200,000 of bitcoin to regain access to research and recover its commercial operations and the University of California, San Francisco that paid attackers $1.14 million to recover hacked data from its School of Medicine (Haque et al., 2023; Lallie and Titis, 2023; Fouad, 2021), University of Utah paying $457,000, and the University of California paying $1.14 million in 2020 (Fouad, 2021). As in Regis University's case, ransom

payment does not guarantee a return to complete system restoration, which had day-to-day operational disruption for months after paying a ransom (Lallie and Titis, 2023).

It is estimated that ransomware attacks against education increased from 6 per cent in 2019 to 15 per cent in 2020, whereas in healthcare, they increased from 21 per cent to 23 per cent during the same period (Fouad, 2021). Ransomware is typically delivered through phishing emails, malicious attachments, or compromised websites. It can also be spread through malicious emails or social media links.

Critical Comparison of Prior Work

Earlier studies such as Malasowe et al., (2024) and Armas and Taherdoost (2025) emphasized that HLI underperform in cybersecurity maturity compared to corporate organizations, largely due to underinvestment and poor Governance. Similarly, Nkambule and Vuuren, (2024) linked cybersecurity maturity with digital transformation and argued that risk assessment frameworks must be integrated into broader governance structures. More recent works (Ulven and Wangen, 2021; Yusif & Hafeez-Baig, 2023) have shown that universities face a distinct challenge of balancing openness and academic freedom with the need for robust information security controls. Compared to these prior works, the research provides valuable quantitative insights into maturity levels. It reaffirms challenges in Governance, human factors, and technical limitations.

METHODOLOGY

Research Design

This study employed a descriptive research design to assess the state of cybersecurity maturity in universities. The design was appropriate for capturing current practices, policies, and perceptions related to cybersecurity across multiple institutions.

Target Population and Sampling

The target population comprises IT personnel and system administrators responsible for information systems security in 25 accredited universities in Nairobi County, Kenya. A purposive sampling technique selected respondents with relevant knowledge and responsibilities in cybersecurity governance, implementation, or oversight. The sample size was calculated using the Raosoft Online Calculator (http://www.raosoft.com/samplesize.html), where the confidence level is 95%. The sample size of 176 IT staff satisfied the sample size requirement for an online survey. According to this formula, 176 responses are sufficient for a quantitative study and for an unknown population when the hypotheses are tested based on the proportion of the population, which is expressed as 0.5 (50%) with 95% internal confidence and a margin of error of 5% (0.05). The sampling frame is shown in Table 1 below:

Table 1: sampling frame

University Category	No. of Universities	The population of IT Staff	Population Proportion (%)	Sample size
Public	3	180	56	99
Private	22	141	44	77
Total	25	321	100	176

Data Collection Methods

Primary data was collected using a structured online questionnaire to evaluate cybersecurity maturity across three dimensions: institutional Governance, technical capacity, and human factors. To ensure academic rigor, the instrument was adapted from the National Institute of Standards and Technology (NIST) Cybersecurity Framework, which is widely recognized as a standard for assessing cybersecurity maturity. This alignment with an established framework enhanced the validity of the tool, ensuring it measured what it intended to assess.

Before deployment, the questionnaire underwent pre-testing (pilot testing) with a small sample of respondents to identify potential ambiguities, test the items' reliability, and confirm the questions' clarity. Adjustments were made based on feedback to improve readability, reduce bias, and enhance consistency in responses.

Data Analysis

Collected data were cleaned and coded, then analyzed using Statistical Package for the Social Sciences (SPSS). Descriptive statistics, including frequencies, means, and percentages, were used to interpret the maturity levels of various cybersecurity domains. For clarity, the results were presented using tables and charts.

Ethical Considerations

Several ethical considerations were adhered to during data collection and model testing. The researcher obtained authorization that furthered the purpose of the study. The ethical considerations are in line with the requirements of the regulating authorities. For data to be collected from universities, consent was obtained from the institutions. This was done according to the institution's regulations, requiring an introductory letter from the School of Graduate Studies and a permit from the National Commission for Science Innovation and Technology (NACOSTI). Informed consent is critical in research with participants (Moore, McArthur, & Noble-Carr, 2018). We, therefore, ensured the study participants confirmed their consent and overall willingness to contribute, as expressed through their review of the consent form and subsequent active participation. The consent form was clear, detailed, and understandable to the potential research participants (Clark, 2019).

RESULTS

Has your Institution been a victim of a cyber-attack?

The respondents were asked to specify if their institution had been a victim of a cyber attack. 57% of the respondents indicated they had been victims of cyber attacks, while 43% said no, as shown

in Table 2. Cyber-attacks are a prevalent reality for institutions in this study, with a majority (57%) confirming victimization. This high incidence rate highlights critical vulnerabilities and underscores an urgent need for proactive cybersecurity measures across the sector. The 43% reporting no attacks may benefit from risk assessments to determine whether this reflects robust defences or undetected breaches.

Table 2: Has your Institution been a victim of a cyber-attack?

Variable	Frequency	Percent
Yes	88	57
No	66	43
Total	154	100.0

Types of Cybersecurity Attacks

The data reveals that phishing is the most widespread cyber threat among higher learning institutions, with 96.1% (148 out of 154) of respondents confirming its occurrence. Ransomware follows closely, reported by 89% (137 respondents), indicating its significant impact on institutional systems. DDoS attacks were experienced by 78.7% (129 respondents), highlighting the frequent disruption of online services. In contrast, internal threats were less common, reported by 33.1% (51 respondents), though still notable due to their potential damage from within the institution.

Physical system attacks were rare, with only 5.8% (9 respondents) affected, and just 1.3% (2 respondents) reported experiencing other cyber-attacks. The data suggests that most institutions face multiple cyber threats, with phishing, Ransomware, and DDoS being the most prevalent. This indicates a pressing need for stronger cybersecurity awareness, improved technical defenses, and formal governance structures to mitigate external and internal threats. These findings are presented in Table 3 below.

Table 3: Types of Cybersecurity attacks

Variable	Yes	No	Total
Phishing	148	6	154
Ransomware	137	17	154
Internal threats	51	103	154
DDoS	129	35	164
Other	2	152	154
Physical Systems Attack	9	145	154

Frequency of Attacks

Participants were asked to indicate how often their institutions experienced cyber attacks. The results showed that 21% reported attacks occurring annually, and another 21% weekly. Monthly attacks were noted by 18% of the respondents, while 19% stated that their institutions had not experienced any attacks. Although 19% claimed no attacks, this could imply strong cybersecurity controls, limitations in detecting threats, or possible underreporting, raising concerns about monitoring effectiveness and the openness of institutional disclosures.

The high rate of reported attacks, such as the 21% experiencing them weekly, correlates with known deficiencies in cybersecurity governance, including the absence of formal risk management frameworks in 55% of institutions and limited vulnerability scanning, which 17% perform only once a year. These findings underscore how structural weaknesses contribute to increased risk exposure. Moreover, the "Other" category (21%) reflects a lack of standardized metrics for logging cyber incidents, complicating efforts to analyze and coordinate responses at a sector-wide level. Institutions reporting no attacks may lack the tools or expertise to detect breaches, echoing earlier concerns over limited internal cybersecurity capabilities. This reinforces the need to investigate the socio-technical factors behind underreporting, including fears of reputational damage or resource limitations. The data highlights widespread Vulnerability to cyber threats across higher learning institutions (HLIs). This may indicate shifting threat patterns or inconsistencies in how incidents are reported. These findings are summarized in Table 4.

Table 4: Frequency of Attacks

Variable	Frequency	Percent
Weekly	79	21
Monthly	69	18
Annually	79	21
None	74	19
Other	83	21
Total	384	100.0

Cybersecurity Strategies Put in Place

As shown in Table 5, the data highlights the distribution of cybersecurity measures implemented by higher learning institutions. The most adopted control is Securing Active Directory (AD), with 18% (27 respondents) indicating its use, focusing on managing user access and identity within institutional networks. Multi-factor Authentication (MFA) follows at 17% (26 respondents), showing increasing awareness of securing access points through layered authentication mechanisms.

Intrusion Detection and Prevention Systems (IDPS) were reported by 14% (21 respondents), indicating some level of network monitoring. In comparison, Backup Systems and Antivirus Software received 12% (19 responses), emphasizing data protection and malware defense equally. Despite being a fundamental line of defense, firewalls were reported by only 11% (17 respondents), which may suggest underutilization or outdated implementations.

Alarmingly, User Awareness Programs were cited by only 8% (13 respondents), pointing to a major weakness in addressing the human element of cybersecurity. An additional 8% (12 respondents) reported using other unspecified methods, which may include ad hoc or institution-specific tools.

The data shows that while technical measures like access control, MFA, and antivirus software are in place, the low prioritization of user awareness exposes institutions to significant risks, particularly from social engineering and phishing attacks. Institutions appear to be more invested in technical defenses than in developing a cyber-aware culture, which is essential for holistic resilience. To improve cybersecurity maturity, there is a need for balanced investment in technical and human-focused strategies, emphasizing staff training, awareness campaigns, and policy enforcement.

Table 5: Cybersecurity Strategies Put in Place

Variable	Frequency	Percent
Securing AD	27	18
Multi-factor Authentication	26	17
Intrusion Detection/Protection	21	14
Backup System	19	12
Antivirus Software	19	12
Firewalls	17	11
User Awareness	13	8
Others	12	8
Total	154	100.0

How Concerned is the Institution about Cybersecurity?

The data reflects the varying levels of concern regarding cybersecurity among stakeholders in HLIs. A combined 43% of respondents reported being either "Very Concerned" (25%) or "Extremely Concerned" (18%), indicating that a significant portion of institutions acknowledge the seriousness of cyber threats and may be more inclined to invest in protective measures.

However, 21% identified as "Moderately Concerned", suggesting some awareness but possibly lacking urgency or resources to act decisively. Notably, a combined 36% expressed low concern, with 19% being "Slightly Concerned" and 17% stating they were "Not at all Concerned". This

sizeable portion indicates a worrying level of complacency within over a third of institutions, despite the increasing global cyber risks faced by educational environments.

The wide distribution of concern levels highlights inconsistencies in institutional prioritization of cybersecurity. While some HLIs recognize cyber threats as strategic risks, others remain indifferent, potentially due to a lack of awareness, expertise, or resource constraints.

The findings reveal a fragmented perception of cybersecurity risks across HLIs. The high percentage of respondents who are only slightly or not at all concerned is particularly alarming, given the sensitive academic and research data these institutions manage. This disparity suggests a pressing need for national policy interventions, awareness campaigns, and capacity-building programs to elevate cybersecurity as a strategic priority across all institutions. The summarized results are presented in Table 6.

Table 6: How Concerned Is the Institution about Cybersecurity?:

Variable	Frequency	Percent
Very Concerned	38	25
Extremely Concerned	27	18
Moderately Concerned	33	21
Slightly Concerned	29	19
Not at all Concerned	27	17
Total	154	100.0

Cyber Security Management

The data reveals a significant lack of coordination in how institutions implement cybersecurity management, with responsibilities scattered among various internal and external stakeholders—an indication of broader governance weaknesses. A notable portion of institutions (21%) depend on outsourced cybersecurity specialists, signaling a reliance on external expertise for managing critical security functions. Internally, responsibility is fragmented: 19% of institutions place the duty on IT officers, 16% rely on in-house emergency response teams, and only 15% have dedicated cybersecurity units. Additionally, 11% entrust cybersecurity entirely to external service providers.

Alarmingly, 18% of respondents were uncertain about who manages cybersecurity in their institution, reflecting serious organizational ambiguity. The heavy dependence on outsourced experts (21%) and service providers (11%) suggests a systemic overreliance on third parties, which may lead to misalignment with institutional goals and a limited understanding of context-specific risks. This supports earlier findings of disjointed accountability structures and reactive security practices.

The relatively small role of dedicated cybersecurity teams (15%) compared to IT officers (19%) implies that cybersecurity is often viewed as a subset of general IT duties rather than a strategic priority. This approach perpetuates existing skills and resource gaps. 18% of institutions with unclear governance structures for cybersecurity are at risk due to the absence of clearly defined roles, responsibilities, and incident response protocols.

These results are consistent with prior data showing that 55% of institutions lack comprehensive risk management frameworks and 35% outsource their risk assessment, indicative of a reactive and piecemeal approach to Governance. Moreover, this fragmented model contrasts best-practice frameworks like the NIST Cybersecurity Framework (CSF), which advocate for centralized, cross-functional leadership, an element missing in most surveyed institutions. Table 6 presents the detailed findings.

Table 7: Cyber Security Management

Variable	Frequency	Percent
By Service Provider	17	11
Cyber Security Team	23	15
In-House Emergency Team	25	16
IT Officers	25	19
Outsourced Specialist	33	21
Not Sure	27	18
Total	150	100.0

DISCUSSION

Overview of Key Findings

This study examined the cybersecurity maturity of higher learning institutions in Nairobi County, uncovering significant disparities in how institutions manage cyber risks. Ridza et al. (2018) define maturity level as a measure of an organization's or a country's Vulnerability to cyber threats and defense readiness. It provides indicators of how ready an organization or country will react to cyberattacks and what steps to take to alleviate the situation. Additionally, Cybersecurity maturity refers to an institution's preparedness and ability to effectively prevent, detect, respond to, and recover from cyber threats or attacks. It encompasses policies, procedures, technologies, and personnel training programs aimed at ensuring the confidentiality, integrity, and availability of data systems (Kiarie, 2024).

While most have adopted basic technical safeguards such as antivirus software and firewalls, only a small proportion (32%) have formal, documented cybersecurity policies. Furthermore, most

institutions identified human-related aspects such as staff training, awareness, and incident response as the weakest elements. These gaps suggest that although technical defences are present, strategic oversight and human capacity remain underdeveloped.

Kenya's Data Protection Act (2019) and National ICT policies may significantly shape cybersecurity maturity in HLI. The Data Protection Act requires universities to safeguard personal data, appoint Data Protection Officers, and adopt secure data management practices. This compels HLI to formalize policies and improve governance structures, pushing them toward higher maturity levels. National frameworks such as the Kenya National Cybersecurity Strategy and the National ICT Policy (2020) encourage risk assessments, capacity building, and alignment with international standards like ISO/IEC 27001 and NIST. These policies promote structured processes and awareness across academic institutions. However, weak enforcement, limited funding, and inadequate technical capacity constrain full compliance. Many universities struggle to operationalize legal requirements, leading to uneven maturity levels across the sector. In summary, Kenya's legal and policy environment provides the regulatory push for cybersecurity maturity in universities, but actual progress depends on enforcement, resources, and institutional commitment.

Table 8: Cybersecurity Maturity Levels

Table 8 below shows the Maturity level characteristics in HLI.

Maturity Level	Characteristics of Universities	Influence of Legal/Policy Environment
Level 1: Initial (Ad hoc)	Cybersecurity practices are informal and reactive; no structured policies.	Minimal compliance with National frameworks; e.g, Data Protection Act (2019) obligations largely unmet due to lack of awareness or capacity.
Level 2: Developing (Repeatable but Informal)	Some policies exist (e.g., basic IT use guidelines), but implementation is inconsistent.	National ICT Policy (2020) raises awareness of governance requirements; external pressure from regulators pushes universities to adopt baseline practices.
Level 3: Defined (Structured)	Documented cybersecurity policies and governance frameworks in place; conducted partial risk assessments.	Data Protection Act (2019) requires formal data governance structures and appointment of Data Protection Officers; Kenya National Cybersecurity Strategy encourages structured processes.
Level 4: Managed (Integrated)	Cybersecurity is integrated into Governance, budgeting, and compliance processes; regular audits and monitoring are conducted.	Stronger alignment with DPA (2019) compliance (e.g., lawful processing of student/staff data); institutions begin sector-wide collaborations encouraged under national ICT strategies.

Level 5: Optimized (Adaptive)	Continuous improvement, advanced monitoring, and benchmarking against global standards are embedded.	Policies and strategies provide a framework for full integration with international standards (ISO/IEC 27001, NIST CSF); universities actively engage in threat intelligence sharing and research collaborations in line with national cybersecurity objectives.

Relation to Previous Research

The results echo findings from earlier studies that highlight the limitations of relying solely on technology without corresponding Governance and human support. For instance, research by Salam et al. (2025) and Abdullahi (2020) emphasized the importance of integrating organizational policy and user behavior into cybersecurity planning. However, this study offers a unique contribution by focusing on a developing-country context, Kenya, where resource constraints, policy fragmentation, and institutional awareness levels differ significantly from those in high-income settings. Resource scarcity, such as inadequate funding, lack of skilled personnel, and insufficient infrastructure is undoubtedly a key constraint. However, cybersecurity governance challenges in the region are also shaped by factors such as regulatory fragmentation, inconsistent enforcement of national policies, limited regional cooperation, political interference, and competing institutional priorities. Universities may also face political pressures that divert attention and funding away from long-term governance initiatives toward more immediate institutional survival concerns. This highlights the need for **multi-level interventions** including regulatory reform, institutional policy alignment, and capacity building at the leadership level alongside technical and financial investments. In doing so, it fills a critical gap in regional cybersecurity research and offers data-driven insights that are contextually relevant.

Limitations and Shortcomings

Despite its contributions, the study has certain limitations. The data was gathered from a relatively small sample of 25 higher learning institutions, which may limit the generalizability of the findings. Additionally, the reliance on self-reported questionnaires introduces the risk of biased or inaccurate responses, especially if participants were unsure of their institution's cybersecurity posture. Furthermore, the descriptive nature of the analysis does not allow for deeper exploration of causal factors. Future studies could address these limitations by incorporating mixed methods such as interviews, policy document analysis, and system audits to strengthen the validity and reliability of results.

This study deepens the understanding of cybersecurity maturity in higher learning institutions by illustrating the interconnectedness of policy, technology, and human behavior. It challenges the notion that cybersecurity is solely a technical concern and reinforces the need for institutions to adopt comprehensive strategies encompassing governance structures, risk management, and staff development. By doing so, the study aligns with global best practices advocated in frameworks, such as the NIST Cybersecurity Framework, which emphasizes holistic, institution-wide approaches.

Building on these findings, future research could explore the institutional, cultural, and leadership factors influencing cybersecurity decision-making in higher learning institutions. Comparative studies across regions or over time could help identify effective practices and areas requiring improvement. In particular, investigating the role of leadership commitment, organizational culture, and budgetary allocation could shed light on why some institutions are more proactive than others in addressing cybersecurity threats.

The study also opens the door to potential theoretical model developments. One possible model is the proposed "Cyber Security Risk Assessment Model" (CSRA Model), designed for higher learning institutions. This model would assess maturity across five NIST domains and selected PMT, TPB, and GDT IS theories. These theories could be a foundation for future empirical testing and practical implementation.

CONCLUSION

The evaluation of cybersecurity risk posture in HLIs revealed a generally weak to moderate level of preparedness. While cybersecurity awareness is growing, significant gaps exist in Governance, incident response, risk assessment practices, and alignment with standards like NIST and ISO/IEC 27001(Kumar et al., 2024). Many institutions operate without formal cybersecurity policies, structured training, or adequate technical controls (Igbinovia & Ishola, 2023).

HLIs face increasing risks such as data breaches, Ransomware, and phishing attacks, threatening academic data and systems' confidentiality, integrity, and availability. These vulnerabilities pose serious operational and financial challenges, including recovery costs, legal penalties, reputational damage, and disruptions to learning and research activities. Inadequate funding and limited technical capacity further hinder efforts to strengthen cyber resilience.

These findings highlight the urgent need for a tailored cybersecurity risk assessment model to help HLIs identify vulnerabilities, prioritize resources, and build a sustainable defense posture. The insights gathered here provide the foundation for designing and implementing such a model in the subsequent phases of the study (Kumar et al., 2024).

RECOMMENDATION

HLIs represent a unique and complex cybersecurity challenge, combining vast repositories of sensitive data with inherently open academic environments. To strengthen their cybersecurity posture, HLIs should establish dedicated task forces to enforce policies, adopt hybrid risk assessment models tailored to their unique academic environments, and integrate mandatory cybersecurity audits into accreditation processes.

This study recommends that HLIs to adopt a phased, prioritized approach to cybersecurity governance. HLI should begin with low-cost, high-impact measures, such as cybersecurity awareness training, enforcement of basic policies, and designation of a cybersecurity focal person. The next step should involve structured Governance and risk management, including simplified risk assessments and incident reporting mechanisms.

HLIs should progressively invest in affordable technical controls, such as firewalls, endpoint protection, data backups, and network segmentation, while integrating cybersecurity into institutional planning and compliance frameworks like the Kenya Data Protection Act.

The study recommends inter-university collaboration to overcome resource gaps, including creating a shared cybersecurity incident response hub or sector-wide CSIRT to facilitate threat intelligence sharing and coordinated response. Finally, institutions should commit to continuous improvement by benchmarking against international standards (ISO/IEC 27001, NIST CSF) and gradually adopting advanced tools as resources allow.

REFERENCES

Abdullahi Garba, A., Musa Bade, A., Yahuza, M., & Nuhu, Y. (2020). Cybersecurity capability maturity models review and application domain. *International Journal of Engineering & Technology*, *9*(3), 779–784. https://doi.org/10.14419/ijet.v9i3.30719

Aborujilah, A., Al-Othmani, A. Z., Hussien, N. S., Mokhtar, S. A., Long, Z. A., & Nizam, M. (2022). Cybersecurity Risk Assessment Approach for Malaysian Organizations: Malaysian Universities as Case Study. *2022 9th International Conference on Electrical and Electronics Engineering, ICEEE 2022*, 440–450. https://doi.org/10.1109/ICEEE55327.2022.9772546

Alhumud, T. A. A., Omar, A., & Altohami, W. M. A. (2023). An assessment of cybersecurity performance in the Saudi universities: A Total Quality Management approach. *Cogent Education*, *10*(2). https://doi.org/10.1080/2331186X.2023.2265227

Alsulami, M. H., Alharbi, F. D., Almutairi, H. M., & Almutairi, B. S. (2021). *Measuring Awareness of Social Engineering in the Educational Sector in the Kingdom of Saudi Arabia*. 1–13.

Armas, R., & Taherdoost, H. (2025). Building a Cybersecurity Culture in Higher Education: Proposing a Cybersecurity Awareness Paradigm. *Information (Switzerland)*, *16*(5), 1–48. https://doi.org/10.3390/info16050336

Fouad, N. S. (2021). *Securing higher education against cyberthreats : from an institutional risk to a national policy challenge*. https://doi.org/10.1080/23738871.2021.1973526

Ganesen, R., Bakar, A. A., Ramli, R., Rahim, F. A., & Zawawi, M. N. A. (2022). Cybersecurity Risk Assessment: Modeling Factors Associated with Higher Education Institutions. *International Journal of Advanced Computer Science and Applications*, *13*(8), 355–362. https://doi.org/10.14569/IJACSA.2022.0130843

Hina, S., Selvam, D. D. D. P., & Paul Benjamin Lowry. (2019). *Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world*.

Igbinovia, M. O., & Ishola, B. C. (2023). Cyber security in university libraries and implication

for library and information science education in Nigeria. *Digital Library Perspectives*, *39*(3), 248–266. https://doi.org/10.1108/DLP-11-2022-0089

Karbowski, A., & Jaskola, P. (2023). A Markovian Model of Dynamic Cyber Risk Assessment Based on Questionnaires. *2023 16th International Conference on Signal Processing and Communication System, ICSPCS 2023 - Proceedings*. https://doi.org/10.1109/ICSPCS58109.2023.10261162

Kepuska, K., & Tomasevic, M. (2024). A lightweight framework for cyber risk management in Western Balkan higher education institutions. *PeerJ Computer Science*, *10*, 1–23. https://doi.org/10.7717/peerj-cs.1958

Kiarie, N. (2024). Enhancing Digital Resilience: A Cybersecurity Readiness Assessment of Kenyan TVET Institutions. *Journal of the Kenya National Commission for UNESCO*, *5*(1), 1–14. https://doi.org/10.62049/jkncu.v5i1.191

Kioskli, K., & Polemi, N. (2020). *A Socio-Technical Approach to Cyber-Risk Assessment*. *November*.

Kumar, A., Mishra, K., Mahto, R. K., & Mishra, B. K. (2024). *A Framework for Institution to Enhancing Cybersecurity in Higher Education : A Review Un marco institucional para mejorar la ciberseguridad en la enseñanza superior : Una revisión*. https://doi.org/10.62486/latia202494

Lallie, H. S., & Titis, E. (2023). Understanding Cyber Threats Against the Universities, Colleges, and Schools. *Elsevier*.

Malasowe, B. O., Aghware, F. O., Okpor, M. D., Edim, B. E., Ako, R. E., & Ojugo, A. A. (2024). Techniques and Best Practices for Handling Cybersecurity Risks in Educational Technology Environment (EdTech). *Journal of Science and Technology Research*, *6*(2), 293–311. https://doi.org/10.5281/zenodo.12617068

Mantra, I., Abd. Rahman, A., & Saragih, H. (2020). Maturity Framework Analysis ISO 27001: 2013 on Indonesian Higher Education. In *International Journal of Engineering & Technology* (Vol. 9, Issue 2, p. 429). https://doi.org/10.14419/ijet.v9i2.30581

Marican, M. N. Y., Razak, S. A., Selamat, A., & Othman, S. H. (2023). Cyber Security Maturity Assessment Framework for Technology Startups: A Systematic Literature Review. *IEEE Access*, *11*(December 2022), 5442–5452. https://doi.org/10.1109/ACCESS.2022.3229766

Mashila, M., Sithungu, S. P., & Lebea, K. (2025). *Mitigating Ransomware in Government-Managed Institutions : A Global Critical Information Infrastructure Perspective*. 242–248.

Ndeda, L. A., Odoyo, C. O., Systems, I., Town, B., & Town, K. (2019). Cyber Threats and Cyber Security in the Kenyan Business Context. *Global Scientific Journal*, *7*(9), 576–582.

Nkambule, M., & Jansen van Vuuren, J. (2024). Integrating Enterprise Architecture into Cybersecurity Risk Management in Higher Education. *International Conference on Cyber Warfare and Security*, *19*(1), 501–510. https://doi.org/10.34190/iccws.19.1.2189

Pillay, A. K., & Sharma, N. A. (2022). Applicable Cyber Security Recommendations to Prevent Cyber Attacks in Universities. *2022 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*, 1–5. https://doi.org/10.1109/CSDE56538.2022.10089360

Ridza, N. M., Aziz, N. A., Saidin, A. Z., Wahiddin, M. R., Dahlan, A. R. A., Ibrahim, J., & Osman, R. A. H. (2018). Cyber security maturity model and maqasid al-shari'ah. *Proceedings - International Conference on Information and Communication Technology for the Muslim World 2018, ICT4M 2018*, 266–271. https://doi.org/10.1109/ICT4M.2018.00056

Salahdine, F., Mrabet, Z. El, & Kaabouch, N. (2021). Phishing Attacks Detection A Machine Learning-Based Approach. *2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, 250–255. https://doi.org/10.1109/UEMCON53757.2021.9666627

Salam, M., Azmi, K., Bakar, A., Hafizah, A., & Aman, M. (2025). *Building Cyber-Resilient Universities : A Tailored Maturity Model for Strengthening Cybersecurity in Higher Education*. *16*(5), 95–104.

Sharma, A. (2022). Review on Major Cyber security Issues in Educational Sector International Journal of Computer Sciences and Engineering Open Access Review on Major Cyber security Issues in Educational Sector. *International Journal of Computer Sciences and Engineering*, *January*. https://doi.org/10.26438/ijcse/v9i12.2629

Tsen, E., Ko, R. K. L., & Slapnicar, S. (2022). An exploratory study of organizational cyber resilience, its precursors and outcomes. *Journal of Organizational Computing and Electronic Commerce*, *32*(2), 153–174. https://doi.org/10.1080/10919392.2022.2068906

Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet*, *13*(2), 1–40. https://doi.org/10.3390/fi13020039

Yousif Yaseen, K. A. (2022). Importance of Cybersecurity in The Higher Education Sector 2022. *Asian Journal of Computer Science and Technology*, *11*(2), 20–24. https://doi.org/10.51983/ajcst-2022.11.2.3448

Yusif, S., & Hafeez-baig, A. (2023). Cybersecurity Policy Compliance in Higher Education : A Theoretical Framework Cybersecurity Policy Compliance in Higher Education : A. *Journal of Applied Security Research*, *0*(0), 1–22. https://doi.org/10.1080/19361610.2021.1989271