Naif Arab University for Security Sciences
Journal of Information Security & Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR
JISCR

Information Security Behavior in Higher Education Institutions: A Systematic Literature Review

Keefa Bwiino[1,2,*], Geoffrey Kituyi Mayoka[1,2], Lawrence Nkamwesiga[3], Makafui Nyamadi[2,4], and Ibrahim Musenze A.[5]

[1]Makerere University Business School, Kampala, Uganda
[2]ICT University, Yaoundé, Cameroon
[3]Muni University, Arua, Uganda
[4]Ho Technical University, Ho, Ghana
[5]Busitema University, Busitema, Uganda

Received 17 Dec. 2024; Accepted 12 Jun. 2025; Available Online 29 Jun. 2025

Abstract

Information security remains a significant concern in higher education, evidenced by the numerous security-related incidents reported over the last decade. This study investigates the vulnerabilities and threats confronting higher education institutions and proposes information security measures to enhance safety. Key vulnerabilities identified include decentralized IT infrastructure, a diverse user base, legacy systems, insider threats, and insufficient investment in information security. Correspondingly, potential threats and attacks on information in HEIs encompass social engineering attacks, distributed denial-of-service attacks, malware, and insider breaches. Furthermore, the findings advocate for the integration of artificial intelligence in information security monitoring, the incorporation of security education into university curricula, and the implementation of multi-faceted information security measures, including technological, organizational, environmental, and human measures, to ensure robust information security protection in HEIs. The study also highlights areas for future research.

I. INTRODUCTION

The widespread adoption of information and communication technologies has become an integral component of any organization today. This is because ICTs serve as enablers for economic, industrial, and educational progress, thereby enhancing digital governance and management capabilities within various sectors [1]. The growing dependence on computers, smart devices, and information systems has led to the emergence of new computing paradigms, such as artificial intelligence, big data, the Internet of Things, pervasive computing, and cloud environments, which require

Keywords Higher education institutions, information security, information security behavior, information security measures, risk, threats, vulnerabilities

Production and hosting by NAUSS

* Corresponding Author: Keefa Bwiino
kbwiino@mubs.ac.ug

doi: 10.26735/YQBX3351

extensive and universal access to computer resources [2].

Furthermore, it is important to note that the accelerated technological advancements of the Fourth Industrial Revolution have profoundly pervaded higher education institutions, necessitating a comprehensive response to the digital transformation of all its aspects [3]. As systems and devices become increasingly interconnected and perform a wider range of functions, the vulnerability to information security weaknesses also increases [4], [5]. This is substantiated by the plethora of security-related incidents that have occurred over the past decade.

Higher education institutions are particularly vulnerable to information security threats due to the complexity of their computing environments, the diverse range of users, and the sensitive nature of the data they handle [6]. These institutions are responsible for safeguarding sensitive information, such as student records, financial data, and intellectual property, while also providing unfettered access to their networks and resources to support teaching, learning, and research [7]. The open and decentralized environment of universities, coupled with the ubiquitous utilization of portable computing devices and the Bring Your Own Device trend, facilitates easier unauthorized access by malicious actors to sensitive institutional data [7], [8], [9].

In recent years, higher education institutions have encountered numerous information security incidents. For instance, the University of Minnesota experienced a database attack on its financial aid applications in 2023. Additionally, Indiana University was found to have stored student data on two unprotected Azure storage blogs, exposing 1.3 million files in May 2023.

Furthermore, the University of Georgia confirmed that cybercriminals had gained unauthorized access to data stored in the MOVEit Secure File Transfer and Automation software, which the university had been utilizing for the storage and transfer of sensitive information, in September 2023. Similarly, in June 2022, the University of Pisa fell victim to the BlackCat ransomware group, which seized the university's IT system and demanded a substantial ransom of $4.5 million, one of the larger ransoms observed in that year.

Other notable cases include the University of California announcing a malicious cyberattack in 2021, where stolen personal data was discovered on the dark web, and a data breach that compromised 44,000 student records at Arden University in 2022 due to human errors. These cybersecurity incidents have occurred globally, with examples from various regions such as the USA, Africa, Asia, and Europe underscoring the pervasive nature of this challenge for higher education institutions [10], [11], [12], [13], [14].

The failure to properly secure information can lead to a range of consequences, including financial losses, diminished institutional performance, intellectual property infringement, and reputational damage [15], [16], [17]. According to the Africa Cyber Security Report 2023, the financial impact of cybercrime was projected to escalate, with global losses estimated to reach USD 8 trillion in 2024 and potentially surpass USD 10.5 trillion by 2025 [18]. Information security incidents have been increasingly reported within the higher education sector, where sensitive data belonging to students, faculty, and staff have been subjected to unauthorized access and exploitation for unlawful ends [8], [9], [19], [20].

Despite the substantial body of research in this domain, a comprehensive and current overview of information security practices and key findings in higher education institutions remains lacking [8]. This review aims to synthesize the extant literature on information security practices within higher education for the past decade to elucidate the critical factors influencing data breach incidents in these institutions and suggest areas for future research.

A prior literature analysis was conducted by Imbaquingo-Esparza et al. [21]. The authors emphasize that higher education institutions must adopt a rigorous approach to information security, which involves implementing comprehensive security policies, deploying robust technical safeguards, and conducting continuous critical security evaluations. While the study has identified security challenges impacting the security measures and tools used by higher education institutions to mitigate security threats, it lacks a more in-depth analysis of the specific vulnerabilities, security priority areas, and security incidents encountered by

these institutions. Additionally, given the evolving nature of the information security landscape and the fact that the study was undertaken two years prior, an updated assessment of information security practices would be beneficial to inform subsequent investigations in this domain. Another literature analysis focused on the factors influencing information security policy compliance behavior in higher education institutions, ignoring other information security practices [22].

Extant literature shows that higher education institutions have compelling reasons to investigate information security management [19], [21]. For instance, universities continuously expand their digital presence, rendering them increasingly vulnerable to cyber threats. Furthermore, universities are characterized as densely populated hybrid settings that foster the digital economy and heavily rely on open-by-design, decentralized, multi-stakeholder, transient, and multi-purpose platforms for instruction, learning, research, and innovation [19].

Furthermore, the existing literature suggests that information security practices in higher education institutions are fragmented and that information security management in this sector remains a highly underexplored topic. While studies have examined cybersecurity risk management frameworks in the context of higher education [23], [24], there is a dearth of comprehensive, systematic reviews that provide a holistic understanding of the information security landscape in this domain. Accordingly, in light of prominent systematic literature reviews that have addressed factors influencing cybersecurity and underscored the scarcity of studies examining such factors in higher education, this systematic review aims to answer the following research questions:

- ***RQ1***. What institutional or contextual factors are associated with increased susceptibility to information security threats in HEIs?
- **RQ2.** How do the frequency and severity of cyberattacks on HEIs vary over time, and what patterns emerge in HEIs?
- ***RQ3***. Which categories of information security measures are most effective in reducing security breaches in HEIs?

To answer the research questions above, this paper presents findings from a systematic review of 89 academic publications addressing information security challenges and practices in higher education. The review examines the current state of research on information security in higher education institutions, focusing on security practices and research methodologies, and encompasses literature published from 2014 to the present day.

This study synthesizes prior empirical and conceptual research to examine key factors significantly impacting information security practices within higher education institutions. It also identifies additional variables explored in the research domain, establishes best security practices and measures, highlights gaps in existing literature, and provides recommendations to guide future scholarship. The insights can inform managers and practitioners in academia to enhance security-related behaviors, as well as assist researchers in advancing the body of knowledge on information security in these organizational settings.

II. Methodology

To synthesize and expand the existing knowledge base, this study's research design entails a two-pronged approach to build upon the existing knowledge base. First, a systematic literature search is conducted to uncover relevant scholarly sources, as the rigor of a literature review hinges on the quality of the search process [25], [26]. Second, the retrieved articles are analyzed using predefined criteria to extract the key themes, knowledge gaps, and future research directions.

A. Literature Search Process

This study employed the structured approach outlined by [27] to provide a comprehensive overview of information security practices in higher education institutions. Rigorous literature search guidelines suggested by stress the importance of high accuracy and quality of the literature collected for the review, which enables the identification of genuine research gaps rather than replicating existing

studies. This, in turn, facilitates the formulation of better-informed and more precise hypotheses and research questions, thereby enhancing the overall quality of scholarly work within the community [26]. In our case, the validity and accuracy of this review are contingent upon the selected databases, publications, time frame, keywords employed, inclusion and exclusion criteria, and the application of forward and backward search strategies.

To fulfill the requirements of a thorough and rigorous search, we conducted a comprehensive review across ten prominent academic databases: ScienceDirect, IEEEXplore, JSTOR, SpringerLink, ACM Digital Library, Wiley Online Library, Emerald Insight, Taylor & Francis Online, and Sage Journals. The search queries were formulated to capture relevant scholarly publications addressing information security management in the context of higher education institutions. The keywords employed encompassed a combination of terms such as "higher education," "cybersecurity," "information security," "data breaches," "risk management," and "security practices." The search term comprised search strings as follows;

Search keywords: ({higher education institutions} AND {cybersecurity}) OR ({higher education institutions} AND {information security}) OR ({higher education institutions} AND {data breaches}) OR ({higher education institutions} AND {risk management} OR ({higher education institutions} AND {security practices})

The review followed the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines to ensure methodological transparency and reproducibility

The inclusion criteria for this review required that studies:

a) **explicitly addressed information security or cybersecurity practices within higher education institutions,**
b) **were published between 2014 and 2025,**
c) **were peer-reviewed academic publications (empirical or conceptual),**
d) **were published in English, and**
e) **were accessible in full-text format.**

Studies were excluded if they:

a) **focused on non-academic domains,**
b) **did not directly address HEIs,**
c) **were not written in English,**
d) **were review or secondary studies**
e) **lacked relevance to the review objectives,**
f) **provided insufficient methodological detail or data.**

B. Filtering Criteria as per the PRISMA

1. **Screening based on titles and abstracts:** The review process involved carefully screening the titles and abstracts of the retrieved publications to identify only those that explicitly addressed information security practices within higher education institutions. Studies focused on information security in domains other than higher education were excluded from the analysis. Ultimately, 24 articles were deemed ineligible and subsequently removed from the final sample based on this criterion.
2. **Final eligibility criteria:** This systematic review comprehensively examined scholarly literature investigating the vulnerabilities, cybersecurity threats, and security practices adopted by higher education institutions. Irrelevant studies were excluded from the final analysis phase. This involved rejecting one article due to non-English content, four articles identified as secondary literature reviews, and 29 articles that did not align with the study's objectives. In total, 34 articles were excluded during this screening process.

To further enhance the comprehensiveness of the review without sacrificing its timeliness, we employed the backward snowballing technique [28], [29]. This approach involved systematically examining the reference lists of the selected articles to identify and incorporate additional relevant studies that may have been overlooked in the initial search. This systematic review analyzed a final set of 32 articles that discussed information security practices in higher education institutions. Details are provided in Table I.

As illustrated in Fig. 2, the concept map synthesizes the key areas of focus examined by researchers in the domain of information security practices

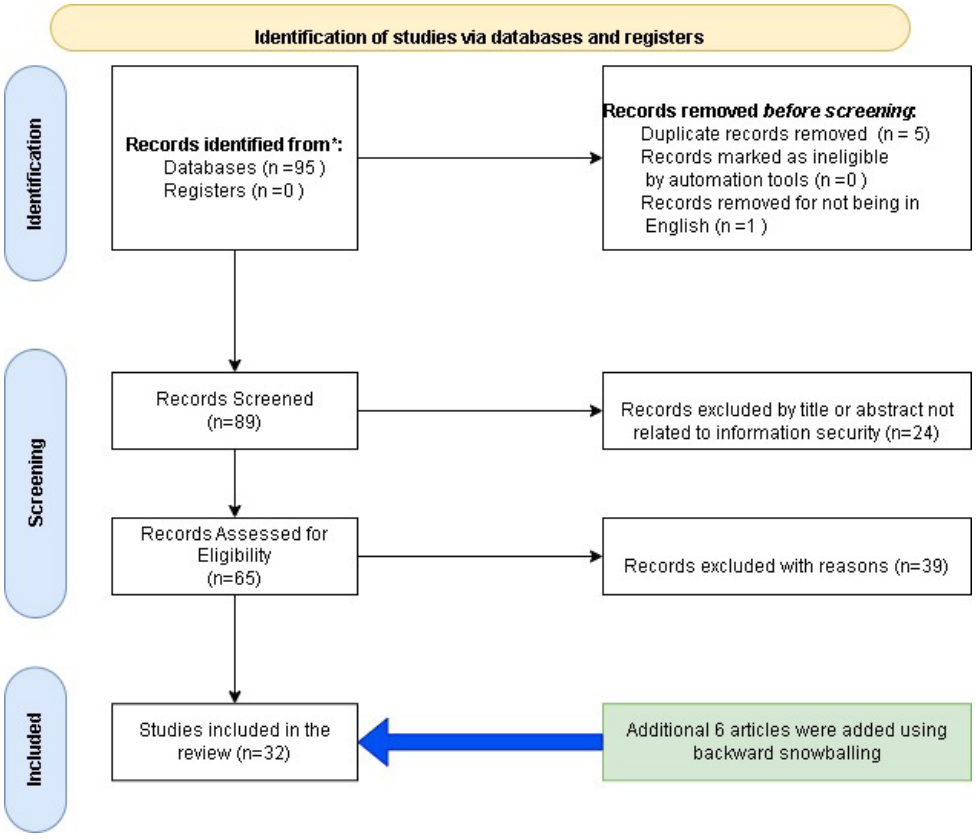

Fig. 1. Selection of Articles using PRISMA. Source(s): Author's own creation

TABLE I
DETAILS OF ARTICLES INCLUDED IN THE STUDY

S/N	Author(s)	Title	Source	Ranking & Citation Impact	Year	Country	Methodology	Type of Study
1	bin Md Ajis, A. F., Rohayu, binti A., & Suhaila, binti O	Catalyst of Information Security in Malaysia Higher Learning Institutions	IEEE Xplore	IS =1.54, h-index=13	2020	Malaysia	Qualitative	Conceptual
2	Alshare, K. A., Lane, P. L., & Lane, M. R	Information security policy compliance: a higher education case study	Emerald Insight	JIS=3.6, h-index=57	2018	US	Quantitative	Empirical
3	Arina, AF., & Anatolie, A	Cyber Security Threat Analysis in Higher Education Institutions as A Result of Distance Learning	*International Journal of Scientific & Technology Research*	JIS=0.41, h-index=26	2021	US	Qualitative	Conceptual
4	C, A., Al-Alawi, E. Y., Al-Hidabi, D. A., & Al-Othmani, A. Z.	Exploring Critical Challenges and Factors Influencing E-Learning Systems Security During COVID-19 Pandemic	IEEE Xplore		2022	Malaysia	Qualitative	Conceptual

S/N	Author(s)	Title	Source	Ranking & Citation Impact	Year	Country	Methodology	Type of Study
5	Aborujilah, A., Adamu, J., Mokhtar, S. A., Al-Othmani, A. Z., Al-alwi, E. Y., & Yahya Al-Hidabi, D. A.	CIA-based Analysis for E-Leaming Systems Threats and Countermeasures in Malaysian Higher Education	IEEE Xplore	C, scopus indexed	2023	Malaysia	Qualitative	Conceptual
6	Ahlan, A. R., Lubis, M., & Lubis, A. R.	Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures	Science Direct	Cite Score: 2.1, Scopus indexed	2015	Indonesia	Quantitative	Empirical
7	Al-Ibrahim, M., & Shams Al-Deen, Y.	*The Reality of Applying Security in Web Applications in Education*	IEEE Xplore	N/A	2014	Kuwait	Quantitative	Empirical
8	Canada-Meza, D. D., Prudente-Tixteco, L., Mercado-Hernandez, P. R., Arenas-Hernandez, J. G., & Ugalde-Eduardo, M.	Recommendations of Security Controls Using Threat Modeling in Information Systems in Higher Education Institutions	IEEE Xplore	Scopus, Web of Science, and CORE	2023	Mexico	Qualitative	Conceptual
9	Daneshmandnia, A.	Exploring Information Security Processes Effectiveness in Educational Institutions: Impacts of Organizational Factors	IEEE Xplore	Scopus, Web of Science, and CORE	2023	US	Quantitative	Empirical
10	Flores, P., Farid, M., & Samara, K.	*Assessing E-Security Behavior among Students in Higher Education*.	IEEE Xplore	Scopus, Web of Science, and CORE	2019	UAE	Qualitative and Quantitative	Empirical
11	*Hina, S., & Dominic, P. D. D.*	*Information security policies' compliance: a perspective for higher education institutions*	Taylor and Francis Online	Citescore: 6.6, JIF: 4.2 Scopus and web of science	2020		Qualitative	Conceptual
12	Hina, S., & Dominic, D. D.	*Need for Information Security Policies Compliance: A Perspective in Higher Education Institutions*	IEEE Xplore	Scopus, Web of Science, and CORE	2017	Malaysia	Quantitative	Empirical
13	Hina, S., & Dominic, D. D.	*Information Security Policies: Investigation of Compliance in Universities*	IEEE Xplore	Scopus, Web of Science, and CORE	2016	Malaysia	Quantitative	Empirical

S/N	Author(s)	Title	Source	Ranking & Citation Impact	Year	Country	Methodology	Type of Study
14	Hina, S., Panneer Selvam, D. D. D., & Lowry, P. B.	*Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world*	Elsevier	JIF: 6.6, CS:10.3 Web of science and scopus	2019	Malaysia	Quantitative	Empirical
15	Huerta Suárez, C. I., Toapanta T, S. M., Gómez Díaz, E. Z., Huerta Vélez, A. E., Suarez, C. I., & Vizuete, M. Z.	*Analysis for Information Security in Virtual Environments for a Higher Education Institution*.	IEEE Xplore	Scopus, Web of Science, and CORE	2024	Ecuador	Qualitative	Conceptual
16	Joshi, C., & Singh, U. K.	*Information security risks management framework – A step towards mitigating security risks in the university network.*	Elsevier	JIF: 6.1 CS: 9.9 Scopus and Web of Science	2017	India	Quantitative	Empirical
17	Kam, H., & Katerattanakul, P.	*Information Security in Higher Education: A Neo-Institutional Perspective*	Taylor and Francis Online	N/A	2014	US	Quantitative	Empirical
18	Karabatak, S., & Karabatak, M.	*Information Security Awareness of School Administrators*	IEEE Xplore	Scopus and Web of Science	2019	Turkey	Quantitative	Empirical
19	RUSERE, K., & NGASSAM, E, K.	*Emerging Network Security Issues in Modern Tertiary Institutions*	IEEE Xplore	Scopus and Web of Science	2020	Namibia	Qualitative	Conceptual
20	Moloja, D., Ngqondi, T., & Mpekoa, N.	BYODelving: Unmasking Security Risks in Higher Education Learning Management Systems - A South African Perspective	IEEE Xplore	Scopus and Web of Science	2024	South Africa	Qualitative	Conceptual
21	Musarurwa, S., Gamundani, A. M., & Shava, F. B.	A Review of Security Challenges for Control of Access to Wi-Fi Networks in Tertiary Institutions	IEEE Xplore	Scopus and Web of Science	2017	South Africa	Qualitative	Conceptual
22	Naga, J. F., & Tinam-isan, M. A. C.	Exploring The Influence of Personality Traits on Students' Information Security Risk-Taking Behaviors: A BFI Assessment	Elsevier	CS: 2.1 Scopus and Web of Science	2024	Philippines	Quantitative	Empirical

S/N	Author(s)	Title	Source	Ranking & Citation Impact	Year	Country	Methodology	Type of Study
23	Ndiege, J. R., & Okello, G.	Towards Information Security Savvy Students in Institutions of Higher Learning in Africa: A Case of a University in Kenya	IEEE Xplore	Scopus and Web of Science	2018	Kenya	Quantitative	Empirical
24	Rastenis, J., Ramanauskaitė, S., Janulevičius, J., & Čenys, A.	Credulity to Phishing Attacks: A Real-World Study of Personnel with Higher Education	IEEE Xplore	Scopus and Web of Science	2019	Malaysia	Quantitative	Empirical
25	Rehman, H., Masood, A., & Cheema, A. R	Information Security Management in Academic Institutes of Pakistan	IEEE Xplore	Scopus and Web of Science	2013	Pakistan	Qualitative	Conceptual
26	Rohan, R., Funilkul, S., Chutimaskul, W., Kanthmanon, P., Papasratorn, B., & Pal, D.	Information Security Awareness in Higher Education Institutes: A Work in Progress	IEEE Xplore	Scopus and Web of Science	2023	Finland, Malaysia, Thailand	Qualitative	Conceptual
27	Salem, Y., Moreb, M., & Rabayah, K. S.	Evaluation of Information Security Awareness among Palestinian Learners	IEEE Xplore	Scopus and Web of Science	2021	Palestine	Quantitative	Empirical
28	Setiawan, B., & Rizal, M. A	Measurement of Information Security and Privacy Awareness in College Students after the Covid-19 Pandemic	Elsevier	CS: 2.1 Scopus and Web of Science	2024	Indonesia	Mixed Methods	Empirical
29	Taha, N., & Dahabiyeh, L.	College students information security awareness: a comparison between smartphones and computers.	Springer	JIF: 4.2, CS: 7.8 Web of Science, Scopus	2020	Jordan	Quantitative	Empirical
30	Toapanta, S. M. T., Del Pozo Durango, R. H., Díaz, E. Z. G., Trejo, J. A. O., Gallegos, L. E. M., Arellano, Ma. R. M., Vizuete, M. Z., & Hifóng, M. M. B.	Proposal for a security model applying artificial intelligence for administrative management in a higher education institution	IEEE Xplore	Scopus and Web of Science	2023		Qualitative	Conceptual
31	Kam, H.-J., & Katerattanakul, P.	Information Security in Higher Education: A Neo-Institutional Perspective	Taylor and Francis Online	N/A	2024	USA	Quantitative	Empirical
32	Dioubate, B. M., Daud, W., & Norhayate, W	Cyber Security Risk Management Frameworks Implementation in Malaysian Higher Education Institutions	International Journal of Academic Research in Business and Social Sciences	N/A	2022	Malaysia	Qualitative	Conceptual

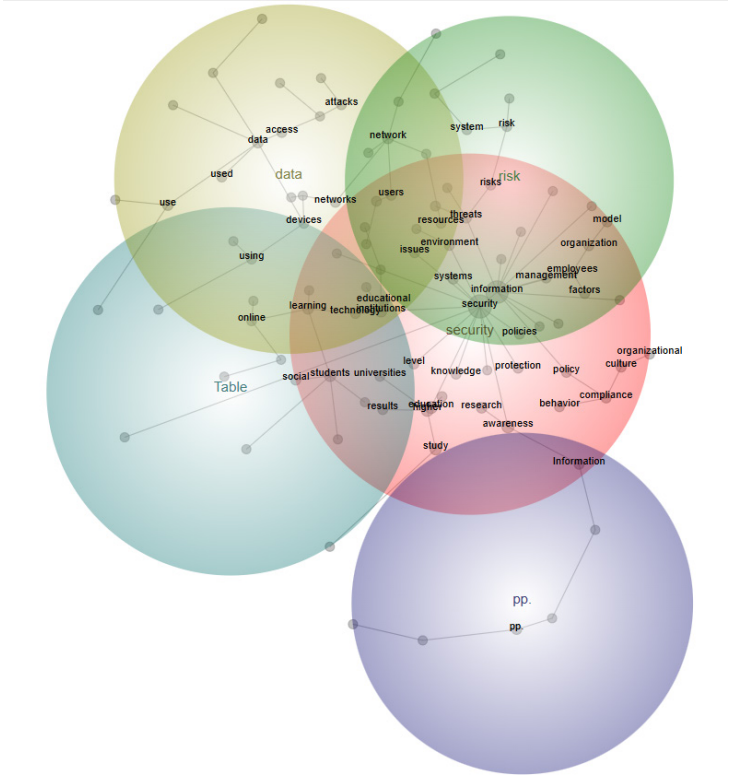

Fig. 2. Concept Map Created using Leximancer. Source: Author's creation

within higher education institutions, utilizing the Leximancer analysis tool. The visual inspection of Fig. 2 identifies data, security, and risk as the main themes mostly examined by the researchers. This points to the need to protect data as a valuable resource by mitigating the risk of data loss or un unauthorized access by ensuring good security measures. The studies emphasize the need for a comprehensive information security approach, encompassing technological, organizational, and environmental measures.

Based on the observations in Table II, this study discerns recurring themes in scholarly research pertaining to information security within HEIs. Moreover, the thematic table elucidates the cybersecurity environment prevalent in higher education institutions, categorizing it by Vulnerabilities (root causes) , Threats (manifestations), and Measures (responses) spanning technological, organizational, and environmental factors. This systematic framework empowers stakeholders to prioritize mitigation strategies efficiently.

C. Information security vulnerabilities, threats, and attacks faced by higher education institutions

1. Vulnerabilities

To answer our first research question, RQ1, this study has identified the following information security vulnerabilities faced by higher education institutions as discussed below:

a) Decentralization, User Diversity, and IT Complexity

The decentralized administrative structures and heterogeneous IT ecosystems in higher education institutions (HEIs) create significant vulnerabilities. Li et al. affirm that these factors hinder centralized control, complicating the deployment of uniform security policies and monitoring [7]. This observation is corroborated by a case study at the University of Manchester, which experienced a ransomware attack attributed to fragmented IT governance and insufficient network segmentation [30].

Empirical data from EDUCAUSE shows that 62% of surveyed institutions acknowledge the lack of centralized IT security management as a

top impediment to effective information security [31]. This contrasts with corporate environments, which often adopt centralized and hierarchical IT governance models that yield higher control and accountability [32], [33]

b) Poor Implementation of Risk Management Frameworks

The ineffective adoption of cybersecurity frameworks and misalignment with international standards such as ISO 27001 and NIST-CSF remain prevalent in HEIs [23], [34]. A comparative study by Singh et al found that only 28% of HEIs in Southeast Asia implement risk management frameworks aligned with ISO 27001, compared to 72% in banking institutions [34]. These discrepancies suggest that higher education institutions lag behind in maturity models of risk governance compared to other critical sectors.

c) Inadequate Investment and Legacy Systems

Accordingly, this study established that HEIs often struggle with constrained budgets, leading to underinvestment in cybersecurity. Studies by Dioubate and Li highlight the persistence of outdated infrastructure, inadequate backup systems, and a lack of employee training on security best practices, which exposes systems to known exploits [23], [7]. For example, the University of Calgary suffered a ransomware attack in 2016 due to unpatched systems; the recovery cost the institution over CAD 20,000 [36]. Surveys by the Ponemon Institute showed that 51% of universities allocate less than 5% of their IT budget to cybersecurity, compared to over 12% in the healthcare sector [37]. This budgetary disparity reinforces the vulnerability of HEIs, making them soft targets for adversaries.

d) Application Security Gaps

Al-Ibrahim and Md Ajis documented widespread web application vulnerabilities, including SQL injection, broken authentication, email exposure, and cross-site scripting in university systems across the Middle East [38], [39]. A similar audit of Angolan universities found that over 70% of its applications failed basic OWASP Top 10 compliance tests, making them susceptible to information leakage and unauthorized access [40].

Additionally, there are other application vulnerabilities stemming from server misconfigurations and coding flaws, such as application error messages, the transmission of user credentials in plain text, the display of error messages on web pages, ASP.NET padding oracle vulnerability, and slow HTTP denial-of-service attacks [38], [40].

e) Insider Threats

The studies synthesized in this review have identified that insiders, such as employees and students, are often the most vulnerable point in safeguarding the organization's data assets [41], [42], [43], [44], [45]. Negligence, malicious motives, or unintentional actions by these individuals can jeopardize the security of sensitive information. Additionally, the lack of comprehensive information security policies, inadequate user awareness, and insufficient investment in security technologies have been highlighted as systemic issues that leave higher education institutions susceptible to cyber threats [41], [43].

Comparative studies reveal that educational institutions are twice as likely as financial institutions to suffer from insider-driven breaches [46]. This is due to the transient nature of student populations and limited identity lifecycle management [41]

D. Information Security Threats

The findings of this study have identified that Higher education institutions have critical data assets that should be protected against information security threats. These include users, web applications, web servers, database servers, databases, document repositories, institutional networks, and the user network [47]. This review has identified the following threats affecting higher education institutions:

1. Phishing:

Phishing scams represent a prevalent threat in higher education, where perpetrators frequently send emails pretending to be legitimate authorities and experts to target university faculty, staff, and students [47], [48], [49]. These fraudulent emails often include links that, when clicked, urge recipients to disclose personal data such as full names, Social Security numbers, birth dates, and financial card information. Criminals then leverage this stolen information to commit identity theft [48].

Studies have established that phishing is the most common cyberattack vector in HEIs [50], [51]. Notable examples of phishing attacks in HEIs include a phishing campaign at the University of California, Irvine, in 2017, where over 1,800 student and faculty accounts were compromised, resulting in unauthorized data access and financial fraud [52], a phishing campaign that compromised dozens of email accounts, leading to unauthorized grade changes and data leaks at the University of Maryland Global Campus, affecting 300,000 students and staff [53]. Furthermore, a study by Diaz et al. [54] revealed that 59% of students had encountered phishing emails, and 17% admitted to falling victim to at least one phishing attempt.

Whereas Lallie et al. [11] highlight the lack of cybersecurity awareness among students as the cause of susceptibility to phishing, Jain et al. [55] focus on the technical aspects of phishing, such as the difficulty in visually distinguishing between legitimate and spoofed websites. And yet Kumar et al. [56] emphasize the organizational challenge of keeping all users informed and vigilant. Therefore, higher education institutions must implement robust detection mechanisms to identify and block malicious emails, as well as conduct regular security awareness training to educate users about phishing tactics and preventive measures [57], [58]

2. Insider threats

Complacent behavior of stakeholders and unauthorized manipulation or tampering of data pose a significant challenge for higher education institutions [49]. Malicious insiders may illicitly access and alter student academic and financial records, leading to data breaches, distortion of institutional records, and financial losses [7], [47]. Insider threats include the following;

Repudiation, which refers to the denial of responsibility by individuals, has been recognized as a substantial challenge in higher education institutions [47]. Universities frequently struggle to implement effective accountability meahsures, which can hinder the successful deployment of information security practices. This is a result of the failure to identify the users on the network arising from so many connections.

Unauthorized access and misuse of confidential information by university personnel, including the inappropriate escalation of user privileges to restricted systems and data [47], [49].

Suboptimal password management practices, including the use of easily guessable passwords, storing passwords in web browsers, maintaining the same credentials for prolonged durations exceeding 30 days, and employing shorter password lengths, can expose the institution's systems to password-cracking vulnerabilities [47], [59]

3. BYOD

Many higher education institutions have implemented new infrastructure to enable students to use their own devices for educational purposes [60]. This poses network security challenges related to the monitoring of mobile devices accessing the institution's Wi-Fi networks [61]. The Bring Your Own Device model exacerbates endpoint vulnerabilities, as users sometimes alter institutional security settings on their devices to access restricted websites and unsecured public wireless networks [49], [64], [65]. This is because personal devices utilized by students and faculty often lack the same robust security safeguards and controls that are typically implemented on institutional-owned equipment [49], [62].

A case in example case was at Tshwane University of Technology, where devices infected with malware through public Wi-Fi were reportedly responsible for a minor ransomware outbreak [64]. Compared to regulated industries like banking, where device policies are strictly enforced, HEIs rarely impose stringent endpoint protection protocols, creating exploitable gaps [45].

4. Distributed Denial of Service Attack (DDOS).

These attacks seek to overwhelm websites or networks, impairing their performance or rendering them entirely unavailable to users. Bondoc et al. [34] reported DDoS attacks that crippled university servers in the Philippines, delaying examinations and online registration. Canada-Meza et al. [47] reiterate how HEIs' reliance on cloud and online services makes them attractive targets for such resource-exhaustion attacks.

The education sector is a frequent target of distributed denial-of-service attacks, ranking among

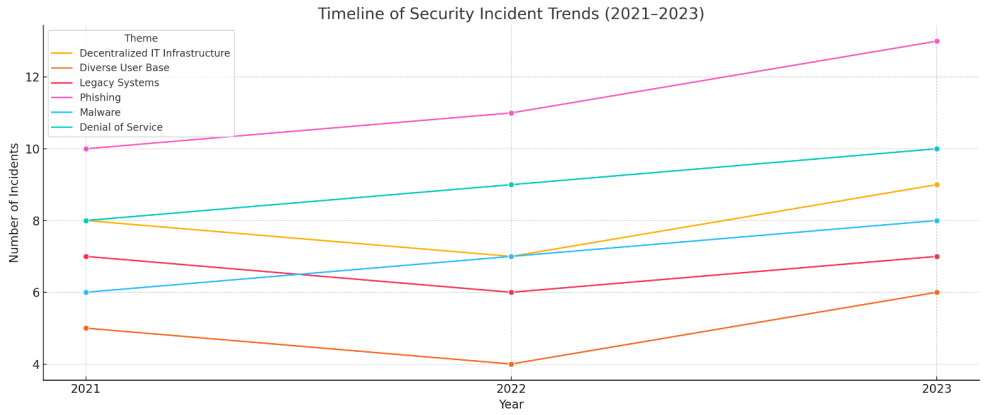

Fig. 3. Security Incident Trends (2021 –2023)

the top three globally according to Cloudflare, with ideological or competitive factors often serving as the impetus. A study by Kaspersky reported a 350% increase in DDoS attacks targeting educational resources in 2020 compared to 2019, with much of the increase attributed to distance learning services [65].

5. Malware

Higher education institutions also grapple with the threat of ransomware [34], [66], which can compromise critical functions and jeopardize the confidentiality of sensitive information. Flores et al. [68] observed that HEIs experienced a 300% increase in ransomware attacks between 2017 and 2019. The 2020 ransomware attack on Maastricht University forced the institution to pay €200,000 in bitcoin to regain access to its systems [67]. These attacks often exploit misconfigured servers or phishing vectors.

As observed from Fig. 3 above, Research findings from this study suggest a consistent upward trend in the frequency of security incidents within HEIs. Phishing attacks represent the most common type of security incident, followed by denial-of-service attacks and malware. The decentralized IT infrastructure poses the most substantial vulnerability leading to these security incidents, followed by the presence of outdated systems incapable of effectively addressing contemporary cyber threats and the heterogeneity of the user base. This answers our first research question, RQ1.

III. Information Security Measures Implemented to Ensure Information Security in Higher Education Institutions

This study has established that achieving robust information security in higher education institutions requires a multifaceted approach that examines the interplay of technological, organizational, and environmental factors [39], [41], [42], [44], [68]. This holistic perspective can help identify the most significant determinants for safeguarding critical data assets.

A. Technological Measures

Higher education institutions can leverage a variety of technological safeguards to secure their digital assets. These include cryptographic techniques such as encryption, hashing, and digital signatures, as well as intrusion detection systems, firewalls, regular data backups, identity management, and access control mechanisms [39], [68], [69]. Additional security measures encompass password management, multi-factor authentication (e.g., security questions, token-based, biometrics), spam filtering, updated antivirus software and systems, use of secure protocols, and digital watermarking, [43], [69], [70]. Additionally, this study also established that an AI-powered security framework, engineered to identify irregularities and recognize prospective threats, can serve as a beneficial technological approach to bolster information security within higher education establishments [71].

Institutions like the University of Cambridge have adopted artificial intelligence-driven intrusion detection systems, significantly reducing false

positives in real-time threat detection [71]. However, smaller institutions in Africa and Southeast Asia often rely on signature-based antivirus tools, which fail to detect zero-day attacks [72].

While encryption and multi-factor authentication are standard in banks and healthcare, only 40% of HEIs implement MFA, leaving a large segment of users unprotected [71]. Multi-factor authentication is an excellent tool to combat the most common attacks, as it involves verifying the end user's identity. In MFA, users' identities are validated through the combination of two or more factors to grant access to services or data [73].

Multi-factor authentication adds layers of security to the authentication process by requiring users to provide multiple verification factors to gain access. By using a combination of authentication schemes, security can be enhanced [74]. In particular, multi-factor authentication can be deployed to reduce the risk of phishing and identity theft [75].

B. Organizational Measures

The literature indicates that higher education institutions can bolster their information security posture through various organizational initiatives [39], [68]. The studies synthesized in this study revealed that the organizational components of information security address the administrative facets of an organization.

These include executive support, centralized IT governance, continuous security audit [76], [77], [78], implementing security education, training, and awareness programs (SETA) [24], [43], [49], [63], [79], [80], [81], developing and enacting information security policies, fostering an information

TABLE II
THEMATIC TABLE FOR THE VTC FRAMEWORK

Theme	Sub-Themes	Study (Citation)
Vulnerabilities	**1.** Decentralized networks, Complex IT infrastructure, and User diversity **2.** Poor Risk Management Implementation **3.** Lack of Security Investment and Legacy Systems **4.** Application Security Gaps **5.** Insider Weaknesses	[7], [23], [30], [31], [32], [34], [35], [37], [38], [39], [40], [41], [42], [44], [45], [67]
Threats	**1.** Malware **2.** Phishing **3.** BYOD **4.** DDoS attacks **5.** Insider threats **6.** Ransomware	[7], [11], [34], [45], [47], [48], [49], [55], [56], [59], [61], [62], [63], [65], [66], [50]
Technological Countermeasures	**1.** Encryption **2.** Intrusion Detection Systems (IDS) **3.** Firewalls **4.** MFA **5.** AI threat detection **6.** Access control	[39], [43], [68], [69], [70], [71], [73], [74]
Organizational Countermeasures	**1.** Centralized governance **2.** Security audits **3.** SETA programs **4.** Risk management **5.** Leadership involvement	[39], [41], [43], [44], [45], [49], [63], [76], [78], [80], [81], [82], [83]
Environmental Countermeasures	**1.** ISO/COBIT/NIST/ITIL compliance **2.** External audits **3.** Adherence to global standards	[39], [84], [85]

security culture within the institution like enforcement of password policies, adopting risk management practices, separation of personal digital devices from institutional devices [41], [42], [45], [49], [59], [69], [77], [82], and aligning procedural activities, security initiatives, and the commitment of personnel across all levels, from senior leadership to frontline staff [39], [45], [83].

Institutions with centralized IT governance models, such as MIT, have demonstrated superior incident response times and lower breach impacts [82]. A study by Liu et al. [80] confirms that institutions with established SETA programs show 45% fewer successful attacks than those without.

Despite the evidence, Ndiege et al. [83] found that only 33% of East African universities conduct regular security audits, weakening their security maturity compared to their Western counterparts.

C. Environmental measures

The findings of this study underscore the importance of higher education institutions aligning their security practices with internationally recognized information security management frameworks, such as ISO 27000, COBIT, ITIL, NIST, and EDUCAUSE, to ensure adherence to industry standards and best practices [39], [84], [85]. While positive outcomes are observed from compliance (e.g., improved auditability and staff accountability)

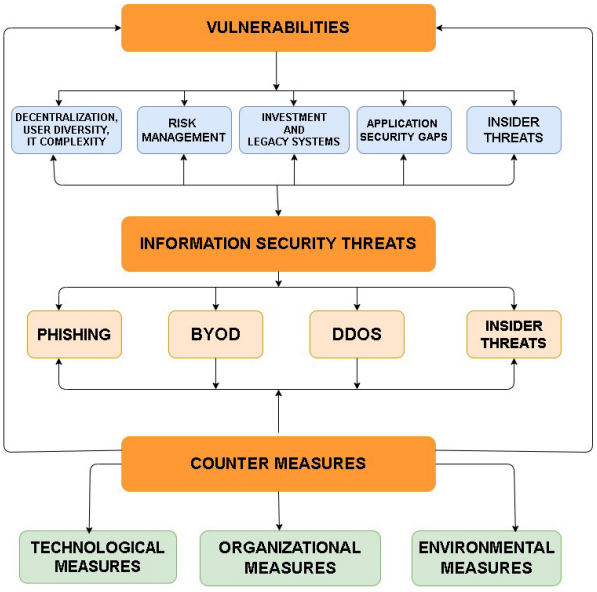

Fig. 4. Vulnerabilities, Threats, Countermeasures (VTC) Framework. Source: Systematic Literature Review

[50], many HEIs consider such compliance too costly or bureaucratic. A survey by EDUCAUSE in 2022 showed that only 23% of member institutions had achieved full ISO certification [31].

Additionally, this review established that external audits are highly influential in information security effectiveness in higher education institutions.

IV. Conceptual Framework

In light of the preceding analysis, this research introduces a conceptual framework designed to elucidate and tackle information security challenges within higher education institutions. This framework integrates three fundamental dimensions: vulnerabilities, threats, and countermeasures. Its purpose is to outline how institutions can effectively mitigate information security risks in increasingly complex academic settings.

A. Description of the Conceptual Framework

1. Vulnerabilities

The framework shows that internal weaknesses exist within an institution's environment that threats can exploit, creating entry points for those threats. These weaknesses can be categorised as lack of central control and standardization, poor risk management implementation, poor investment in security and legacy systems, application security gaps, and insider weaknesses.

2. Threats

Threats represent the external or internal actions that exploit institutional vulnerabilities. The framework captures both technical threats (e.g., malware, phishing, DDoS attacks, ransomware) and human-centered threats (e.g., insider threats, social engineering, negligence). The dynamic interaction between threats and vulnerabilities is a key focus of the model, highlighting how common attack vectors emerge from predictable weaknesses in the HEI environment.

3. Countermeasures

This layer forms the **response mechanism** to both vulnerabilities and threats. It is subdivided into three categories:

- **Technological Measures**: Encompass encryption, intrusion detection systems (IDS), firewalls, multi-factor authentication

(MFA), artificial intelligence-powered threat monitoring, and regular system updates. These tools are aimed at hardening IT infrastructure and reducing system exploitation risks.

- **Organizational Measures**: Focus on strengthening institutional governance. These include centralized IT management, risk assessment procedures, the implementation of information security policies, periodic audits, security education and training programs (SETA), and cultivating a culture of information security from leadership to end-users.
- These are broader strategic actions that ensure institutional alignment with global best practices. They include compliance with frameworks like ISO 27001, NIST, COBIT, and ITIL, as well as participation in external audits and regulatory benchmarks that promote accountability and maturity in information security management.

Interconnection of Elements of the VTC framework

The framework demonstrates that countermeasures should be tailored to directly address specific vulnerabilities and threats, emphasizing a targeted and efficient security posture. For example, phishing threats and weak passwords are mitigated through MFA and SETA programs, while infrastructure vulnerabilities are countered through cloud backups and system upgrades.

Moreover, the inclusion of AI and machine learning-based tools reflects an emerging dimension of proactive security monitoring and threat prediction. Institutions that deploy AI-enhanced solutions can better anticipate, detect, and neutralize complex cyber threats, especially zero-day exploits and advanced persistent threats (APTs).

Importance of the VTC framework

This framework is likely to support policymakers, ICT administrators, and academic leaders in:

- Diagnosing institutional security weaknesses,
- Designing effective and resource-sensitive mitigation strategies,
- Aligning institutional practices with global security standards, and
- Enhancing resilience in the face of evolving cyber risks.

V. Conclusion

The systematic literature review has revealed several important insights regarding the state of information security practices in higher education institutions.

Firstly, the review has highlighted the unique challenges that higher education institutions face in safeguarding their information assets. These institutions are inherently open and collaborative environments, with diverse stakeholders, including students, faculty, and staff, who require access to a wide range of information resources in a highly networked environment. This highly networked open environment, combined with the increasing reliance on technology and the presence of sensitive data, such as student records, intellectual property, and research data, makes higher education institutions particularly vulnerable to cyber threats.

Second, this study has established that the Bring Your Own Device (BYOD) policy adopted by higher education institutions poses the biggest challenge to information security in these institutions. It becomes difficult to control the different devices due to the varying security protocols configured for each device on the network.

Third, the review has identified the need for a comprehensive and strategic approach to information security management in higher education, combining technological, organizational, environmental, and behavioral factors. Many higher education institutions have been found to adopt a reactive and fragmented approach, primarily focusing on technical controls, while neglecting the human, environmental, and organizational factors that contribute to information security risks.

Accordingly, the review has highlighted the crucial importance of fostering a strong information security culture within higher education institutions. Numerous studies have emphasized the critical role of user awareness, training, and engagement in effectively mitigating information security risks [49], [86], [87]. Correspondingly, the review has revealed that incorporating information security education into the curriculum for students at higher education institutions can improve their knowledge and awareness, thereby cultivating an information

security awareness culture that will help mitigate information security risks [87], [88].

VI. Research Gaps and Areas for Future Research

The systematic review has highlighted several promising avenues for future research.

Given the limited empirical evidence regarding the sustained efficacy of particular technological, organizational, or environmental countermeasures within higher education institutions, longitudinal research is warranted to assess the enduring impact of tools such as intrusion detection systems, multi-factor authentication, and security training programs on incident frequencies, regulatory compliance, and user awareness.

Current scholarly work acknowledges the presence of insider threats; however, there is a lack of in-depth investigation into the psychosocial, organizational, and behavioral factors that drive insider misconduct within higher education institutions. Consequently, there is a pressing need for the development of behavioral studies or ethnographic research that examines the motivations, vulnerabilities, and decision-making patterns of insiders, as well as assesses the long-term effectiveness of policies or awareness programs designed to mitigate such threats.

The impact of Bring Your Own Device policies on institutional cybersecurity is acknowledged yet lacks thorough empirical investigation, highlighting the need for case studies or pilot experiments. Such research should assess security settings, network weaknesses, and user adherence within BYOD structures across various higher education institutions.

Despite the widespread recommendation of security education, training, and awareness programs, there is limited empirical evidence regarding the optimal formats, frequencies, and delivery methods. Consequently, further comparative and longitudinal research is needed to evaluate the sustained impact of various training interventions on user behavior and susceptibility to phishing attacks.

Empirical research into the deployment and operational results of AI-driven security tools in higher education is lacking. Consequently, there is a need for more investigation into the challenges of implementation, cost-effectiveness, and accuracy in threat detection of AI frameworks within HEI environments in practice.

The theoretical discourse surrounding international standards such as ISO 27001, NIST, and COBIT lacks empirical evidence regarding their impact on institutional performance following adoption. To remedy this, mixed-method research designs should be employed to assess higher education institutions both before and after the implementation of these compliance standards. This approach would facilitate the evaluation of enhancements in risk management practices, reductions in data breach occurrences, and advancements in overall organizational maturity.

Further research is needed to compare how factors such as institutional size, location, and governance models affect vulnerability and the success of countermeasures. Therefore, cross-national or cross-institutional studies should be conducted to investigate how context-specific factors influence the effectiveness of security frameworks.

During the preparation of this work, the author(s) used the Leximancer tool to visualize the articles and identify the major themes, and also Silvi.ai to sort out the articles with reasons to accept or reject the article as part of the review. After using these tools, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the content of the publication.

Conflict of Interest

The authors declares that there is no conflict of interest.

Funding

The authors of this article did not receive any particular grant from any public, commercial, or not-for-profit funding agency.

References

[1] J. R. C. Nurse, “Cybersecurity Awareness,” in Encyclopedia of Cryptography, Security and Privacy, Berlin, Heidelberg: Springer Berlin Heidelberg, 2021, pp. 1–4. doi: 10.1007/978-3-642-27739-9_1596-1.

[2] Forrester Research, “Insider Threats Drive Data Protection Improvements Threat Detection, Analytics, And Staffing Lead Investment Priorities,” 2021.

[3] M. Alenezi, "Digital Learning and Digital Institution in Higher Education," Educ Sci (Basel), vol. 13, no. 1, p. 88, Jan. 2023, doi: 10.3390/educsci13010088.

[4] T. Nguyen, "Understanding Shadow IT usage intention: a view of the dual-factor model," Online Information Review, vol. 48, no. 3, pp. 500–522, May 2024, doi: 10.1108/OIR-04-2022-0243.

[5] C. T. Do et al., "Game Theory for Cyber Security and Privacy," ACM Comput Surv, vol. 50, no. 2, pp. 1–37, Mar. 2018, doi: 10.1145/3057268.

[6] J. L. Grama and K. Milford, "Ahead of the Curve: IoT Security, Privacy, and Policy in Higher Ed," 2019, pp. 73–86. doi: 10.1007/978-3-030-15705-0_5.

[7] J. Li, W. Xiao, and C. Zhang, "Data security crisis in universities: identification of key factors affecting data breach incidents," Humanit Soc Sci Commun, vol. 10, no. 1, p. 270, May 2023, doi: 10.1057/s41599-023-01757-0.

[8] T. Moletsane and P. Tsibolane, "Mobile Information Security Awareness Among Students in Higher Education : An Exploratory Study," in 2020 Conference on Information Communications Technology and Society (ICTAS), IEEE, Mar. 2020, pp. 1–6. doi: 10.1109/ICTAS47918.2020.233978.

[9] R. De Kock and L. A. Futcher, "Mobile device usage in higher education institutions in South Africa," in 2016 Information Security for South Africa (ISSA), IEEE, Aug. 2016, pp. 27–34. doi: 10.1109/ISSA.2016.7802925.

[10] Z. Scott, "A Recap of Recent Cybersecurity Incidents at Universities." Accessed: Oct. 01, 2024. [Online]. Available: https://www.schellman.com/blog/cybersecurity/cybersecurity-incidents-at-universities-2023

[11] H. S. Lallie, A. Thompson, E. Titis, and P. Stephens, "Understanding Cyber Threats Against the Universities, Colleges, and Schools," Jan. 2023.

[12] R. Marcelo, "2024 State of Ransomware in Education: 92% spike in K-12 attacks - ThreatDown by Malwarebytes." Accessed: Oct. 01, 2024. [Online]. Available: https://www.threatdown.com/blog/2024-state-of-ransomware-in-education-92-spike-in-k-12-attacks/

[13] E. A. Botchway, K. Agyekum, H. Pittri, and A. Lamina, "Deployment of physical access control (PAC) devices in university settings in Ghana," Frontiers in Engineering and Built Environment, vol. 4, no. 1, pp. 1–14, Mar. 2024, doi: 10.1108/FEBE-01-2023-0006.

[14] R. Ganesen, A. A. Bakar, R. Ramli, F. A. Rahim, and M. N. A. Zawawi, "Cybersecurity Risk Assessment: Modeling Factors Associated with Higher Education Institutions," International Journal of Advanced Computer Science and Applications, vol. 13, no. 8, 2022, doi: 10.14569/IJACSA.2022.0130843.

[15] K. Edward, "https://www.upguard.com/blog/top-cybersecurity-problems-for-universities-colleges," Upguard.

[16] H. Cavusoglu, "Economics of IT Security Management," in Economics of Information Security, Boston: Kluwer Academic Publishers, 2004, pp. 71–83. doi: 10.1007/1-4020-8090-5_6.

[17] J. B. Ulven and G. Wangen, "A systematic review of cybersecurity risks in higher education," Feb. 01, 2021, MDPI AG. doi: 10.3390/fi13020039.

[18] "Africa Cyber Security Report," 2023.

[19] I. Bongiovanni, "The least secure places in the universe? A systematic literature review on information security management in higher education," Comput Secur, vol. 86, pp. 350–357, Sep. 2019, doi: 10.1016/j.cose.2019.07.003.

[20] M. B. Muhenda, "The Ugandan Journal Of Management And Public Policy Studies Managing Students' Academic Information: How Are Public Higher Education Institutions In Uganda Prepared To Deal With Internal Cyber-Attacks?," 2018.

[21] D. Imbaquingo-Esparza, J. Díaz, M. Ron Egas, W. Fuertes, and D. Molina, "Information Security at Higher Education Institutions: A Systematic Literature Review," 2022, pp. 294–309. doi: 10.1007/978-3-031-18272-3_20.

[22] A. A. A. Ahmed and H. Abas, "Factors Influencing Information Security Policy Compliance Behavior in High Education Institutions: Systematic Literature Review," Advances in Social Sciences Research Journal, vol. 11, no. 7, pp. 260–273, 2024.

[23] B. M. Dioubate, W. Daud, and W. Norhayate, "Cyber Security Risk Management Frameworks Implementation in Malaysian Higher Education Institutions," International Journal of Academic Research in Business and Social Sciences, vol. 12, no. 4, Apr. 2022, doi: 10.6007/IJARBSS/v12-i4/12300.

[24] S. Hina and D. D. Dominic, Need for Information Security Policies Compliance: A Perspective in Higher Education Institutions. IEEE, 2017.

[25] R. Dekkers, L. Carey, and P. Langhorne, "Quality of Literature Reviews," in Making Literature Reviews Work: A Multidisciplinary Guide to Systematic Approaches, Cham: Springer International Publishing, 2022, pp. 57–105. doi: 10.1007/978-3-030-90025-0_3.

[26] H. Snyder, "Literature review as a research methodology: An overview and guidelines," J Bus Res, vol. 104, pp. 333–339, Nov. 2019, doi: 10.1016/j.jbusres.2019.07.039.

[27] Y. Xiao and M. Watson, "Guidance on Conducting a Systematic Literature Review," J Plan Educ Res, vol. 39, no. 1, pp. 93–112, Mar. 2019, doi: 10.1177/0739456X17723971.

[28] C. Wohlin, M. Kalinowski, K. Romero Felizardo, and E. Mendes, "Successful combination of database search and snowballing for identification of primary studies in systematic literature studies," Inf Softw Technol, vol. 147, p. 106908, Jul. 2022, doi: 10.1016/j.infsof.2022.106908.

[29] M. K. Choong, F. Galgani, A. G. Dunn, and G. Tsafnat, "Automatic Evidence Retrieval for Systematic Reviews," J Med Internet Res, vol. 16, no. 10, p. e223, Oct. 2014, doi: 10.2196/jmir.3369.

[30] JISC, "Cybersecurity Breaches in UK Universities," 2021.

[31] EDUCAUSE, "2022 EDUCAUSE Horizon Report – Information Security Edition," 2022.

[32] J. Abawajy, "User preference of cyber security awareness delivery methods," Behaviour & Information Technology, vol. 33, no. 3, pp. 237–248, Mar. 2014, doi: 10.1080/0144929X.2012.708787.

[33] JISC, "Cyber Security and Universities: Managing the Risk," 2023.

[34] C. E. Bondoc and T. G. Malawit, "Cybersecurity for higher education institutions: adopting regulatory framework," Global Journal of Engineering and Technology Advances, vol. 2, no. 3, pp. 016–021, Mar. 2020, doi: 10.30574/gjeta.2020.2.3.0013.

[35] A. Singh and R. Singh, "Implementation of ISO 27001 in universities: A comparative study," Information Management & Computer Security, vol. 28, no. 1, pp. 44–59, 2020.

[36] BBC, "University pays $20,000 to ransomware hackers - BBC News." Accessed: Jun. 14, 2025. [Online]. Available: https://www.bbc.com/news/technology-36478650

[37] Ponemon Institute, "The Cost of a Data Breach Report," 2021.

[38] M. Al-Ibrahim and Y. Shams Al-Deen, "The Reality of Applying Security in Web Applications in Education," 2014. [Online]. Available: www.conference.thesai.org

[39] A. F. bin Md Ajis, binti A. Rohayu, and binti O. Suhaila, "Catalyst of Information Security in Malaysia Higher Learning Institutions," IEEE, 2020.

[40] E. Mateus and C. Serrão, "Vulnerability Assessment of Angolan University Web Applications," in Proceedings of the 17th International Conference on Web Information Systems and Technologies, SCITEPRESS - Science and Technology Publications, 2021, pp. 518–525. doi: 10.5220/0010716800003058.

[41] K. A. Alshare, P. L. Lane, and M. R. Lane, "Information security policy compliance: a higher education case study," Information & Computer Security, vol. 26, no. 1, pp. 91–108, Mar. 2018, doi: 10.1108/ICS-09-2016-0073.

[42] A. R. Ahlan, M. Lubis, and A. R. Lubis, "Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures," Procedia Comput Sci, vol. 72, pp. 361–373, 2015, doi: 10.1016/j.procs.2015.12.151.

[43] A. Arina and A. Anatolie, "Cyber Security Threat Analysis In Higher Education Institutions As A Result Of Distance Learning," INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, vol. 10, no. 3, pp. 128–133, Mar. 2021.

[44] S. Hina and D. D. Dominic, "Information Security Policies: Investigation of Compliance in Universities," in International Conference On Computer And Information Sciences (ICCOINS), 2016, pp. 564–569.

[45] S. Karabatak and M. Karabatak, "Information Security Awareness of School Administrators," A. Varol, Ed., IEEE, 2019.

[46] DBIR, "DBIR Data Breach Investigations Report," 2022.

[47] D. D. Canada-Meza, L. Prudente-Tixteco, P. R. Mercado-Hernandez, J. G. Arenas-Hernandez, and M. Ugalde-Eduardo, "Recommendations of Security Controls Using Threat Modeling in Information Systems in Higher Education Institutions," in 2023 IEEE International Conference on Engineering Veracruz, ICEV 2023, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/ICEV59168.2023.10329765.

[48] J. Rastenis, S. Ramanauskaitė, J. Janulevičius, and A. Čenys, "Credulity to Phishing Attacks: A Real-World Study of Personnel with Higher Education," in 2019 Open Conference of Electrical, Electronic and Information Sciences, Vilnius, Lithuania, Apr. 2019.

[49] R. Rohan, S. Funilkul, W. Chutimaskul, P. Kanthmanon, B. Papasratorn, and D. Pal, "Information Security Awareness in Higher Education Institutes: A Work in Progress," in 2023 15th International Conference on Knowledge and Smart Technology (KST), IEEE, Feb. 2023, pp. 1–6. doi: 10.1109/KST57286.2023.10086884.

[50] M. Rajab and A. Eydgahi, "Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education,"

Comput Secur, vol. 80, pp. 211–223, Jan. 2019, doi: 10.1016/j.cose.2018.09.016.

[51] H. S. Lallie, A. Thompson, E. Titis, and P. Stephens, "Analysing Cyber Attacks and Cyber Security Vulnerabilities in the University Sector," Computers, vol. 14, no. 2, p. 49, Feb. 2025, doi: 10.3390/computers14020049.

[52] "UC Irvine IT Security Report," 2017.

[53] University of Tennessee Knoxville, "Strengthening Security: Lessons from Recent University Breaches | Office of Innovative Technologies." Accessed: Jun. 14, 2025. [Online]. Available: https://oit.utk.edu/security/learning-library/article-archive/lessons-from-recent-university-breaches/

[54] A. Diaz, A. T. Sherman, and A. Joshi, "Phishing in an academic community: A study of user susceptibility and behavior," Cryptologia, vol. 44, no. 1, pp. 53–67, Jan. 2020, doi: 10.1080/01611194.2019.1623343.

[55] A. K. Jain and B. B. Gupta, "Phishing Detection: Analysis of Visual Similarity Based Approaches," Security and Communication Networks, vol. 2017, pp. 1–20, 2017, doi: 10.1155/2017/5421046.

[56] A. Kumar, K. Mishra, R. Kumar Mahto, and B. Kumar Mishra, "A Framework for Institution to Enhancing Cybersecurity in Higher Education: A Review," LatIA, vol. 2, p. 94, Jan. 2024, doi: 10.62486/latia202494.

[57] K. Omari, "Comparative Study of Machine Learning Algorithms for Phishing Website Detection," International Journal of Advanced Computer Science and Applications, vol. 14, no. 9, 2023, doi: 10.14569/IJACSA.2023.0140945.

[58] R. Shillair, P. Esteve-González, W. H. Dutton, S. Creese, E. Nagyfejeo, and B. von Solms, "Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise," Comput Secur, vol. 119, p. 102756, Aug. 2022, doi: 10.1016/j.cose.2022.102756.

[59] C. Joshi and U. K. Singh, "Information security risks management framework – A step towards mitigating security risks in university network," Journal of Information Security and Applications, vol. 35, pp. 128–137, Aug. 2017, doi: 10.1016/j.jisa.2017.06.006.

[60] M. Limniou, "The Effect of Digital Device Usage on Student Academic Performance: A Case Study," Educ Sci (Basel), vol. 11, no. 3, p. 121, Mar. 2021, doi: 10.3390/educsci11030121.

[61] K. Rusere and E. K. Ngassam, "Emerging Network Security Issues in Modern Tertiary Institutions," in IST-Africa 2020 Conference Proceedings, 2020, pp. 1–9.

[62] D. Moloja, T. Ngqondi, and N. Mpekoa, "BYODelving: Unmasking Security Risks in Higher Education Learning Management Systems - A South African Perspective," in IST-Africa 2024 Conference Proceedings, M. Cunningham and P. Cunningham, Eds., IIMC International Information Management Corporation, 2024, pp. 1–8.

[63] S. Musarurwa, A. M. Gamundani, and F. B. Shava, "A Review of Security Challenges for Control of Access to Wi-Fi Networks in Tertiary Institutions," in IST-Africa 2017 Conference Proceedings, P. Cunningham and M. Cunningham, Eds., IIMC International Information Management Corporation, 2017, pp. 1–8.

[64] I. Myles, "Tshwane University of Technology suffers ransomware attack — thousands of records stolen – MyBroadband." Accessed: Jun. 14, 2025. [Online]. Available: https://mybroadband.co.za/news/security/524680-tshwane-university-of-technology-suffers-ransomware-attack-thousands-of-records-stolen.html

[65] A. Arina, "Network Security Threats to Higher Education Institutions," Central and Eastern European eDem and eGov Days, vol. 341, pp. 323–333, Mar. 2022, doi: 10.24989/ocg.v341.24.

[66] P. Flores, M. Farid, and K. Samara, "Assessing E-Security Behavior among Students in Higher Education," IEEE, 2019.

[67] K. Loohui, "Maastricht University pays €200,000 to Russian hackers | Computer Weekly." Accessed: Jun. 14, 2025. [Online]. Available: https://www.computerweekly.com/news/252477997/Maastricht-University-pays-200000-to-Russian-hackers

[68] A. Aborujilah, E. Y. Al-Alawi, D. A. Al-Hidabi, and A. Z. Al-Othmani, "Exploring Critical Challenges and Factors Influencing E-Learning Systems Security During COVID-19 Pandemic," in 2022 International Conference on Intelligent Technology, System and Service for Internet of Everything (ITSS-IoE), IEEE, Dec. 2022, pp. 1–5. doi: 10.1109/ITSS-IoE56359.2022.9990935.

[69] A. Aborujilah, J. Adamu, S. A. Mokhtar, A. Z. Al-Othmani, E. Y. Al-alwi, and D. A. Yahya Al-Hidabi, "CIA-based Analysis for E-Leaming Systems Threats and Countermeasures in Malaysian Higher Education: Review Paper," in 2023 17th International Conference on Ubiquitous Information Management and

Communication (IMCOM), IEEE, Jan. 2023, pp. 1–8. doi: 10.1109/IMCOM56909.2023.10035569.

[70] C. I. Huerta Suárez, S. M. Toapanta T, E. Z. Gómez Díaz, A. E. Huerta Vélez, C. I. Suarez, and M. Z. Vizuete, "Analysis for Information Security in Virtual Environments for a Higher Education Institution," Institute of Electrical and Electronics Engineers (IEEE), Jul. 2024, pp. 1739–1745. doi: 10.1109/csci62032.2023.00286.

[71] S. M. T. Toapanta et al., "Proposal for a security model applying artificial intelligence for administrative management in a higher education institution," in 2023 International Conference on Computer, Information and Telecommunication Systems (CITS), IEEE, Jul. 2023, pp. 1–5. doi: 10.1109/CITS58301.2023.10188801.

[72] H. Holm, "Signature Based Intrusion Detection for Zero-Day Attacks: (Not) A Closed Chapter?," in 2014 47th Hawaii International Conference on System Sciences, IEEE, Jan. 2014, pp. 4895–4904. doi: 10.1109/HICSS.2014.600.

[73] T. Suleski, M. Ahmed, W. Yang, and E. Wang, "A review of multi-factor authentication in the Internet of Healthcare Things," Digit Health, vol. 9, Jan. 2023, doi: 10.1177/20552076231177144.

[74] I. Velásquez, "Framework for the Comparison and Selection of Schemes for Multi-Factor Authentication," CLEI Electronic Journal, vol. 24, no. 1, Apr. 2021, doi: 10.19153/cleiej.24.1.9.

[75] C. C. Nwoye, "Next-Generation Protection Protocols and Procedures for Securing Critical Infrastructure," International Journal of Research Publication and Reviews, vol. 5, no. 11, pp. 4830–4845, Nov. 2024, doi: 10.55248/gengpi.5.1124.3328.

[76] A. Daneshmandnia, "Exploring Information Security Processes Effectiveness in Educational Institutions: Impacts of Organizational Factors)," in Proceedings of the 2023 IEEE Asia-Pacific Conference on Computer Science and Data Engineering, CSDE 2023, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/CSDE59766.2023.10487771.

[77] S. Hina and P. D. D. Dominic, "Information security policies' compliance: a perspective for higher education institutions," May 03, 2020, Taylor and Francis Inc. doi: 10.1080/08874417.2018.1432996.

[78] C.-W. Liu, P. Huang, and H. C. Lucas, "Centralized IT Decision Making and Cybersecurity Breaches: Evidence from U.S. Higher Education Institutions," Journal of Management Information Systems, vol. 37, no. 3, pp. 758–787, Jul. 2020, doi: 10.1080/07421222.2020.1790190.

[79] S. Hina, D. D. D. Panneer Selvam, and P. B. Lowry, "Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world," Comput Secur, vol. 87, p. 101594, Nov. 2019, doi: 10.1016/j.cose.2019.101594.

[80] J. F. Naga and M. A. C. Tinam-isan, "EXPLORING THE INFLUENCE OF PERSONALITY TRAITS ON STUDENTS' INFORMATION SECURITY RISK-TAKING BEHAVIORS: A BFI ASSESSMENT," Procedia Comput Sci, vol. 234, pp. 527–536, 2024, doi: 10.1016/j.procs.2024.03.036.

[81] J. R. Ndiege and G. Okello, "Towards Information Security Savvy Students in Institutions of Higher Learning in Africa: A Case of a University in Kenya," in IST-Africa 2018 Conference Proceedings, Paul Cunningham and Miriam Cunningham, Eds., IIMC International Information Management Corporation, 2018, pp. 1–8.

[82] H.-J. Kam and P. Katerattanakul, "Information Security in Higher Education: A Neo-Institutional Perspective," Journal of Information Privacy and Security, vol. 10, no. 1, pp. 28–43, Jan. 2014, doi: 10.1080/15536548.2014.912482.

[83] P. Kencana Sari and N. Nurshabrina, "Factor Analysis on Information Security Management in Higher Education Institutions," 2016.

[84] J. Merchan-Lima, F. Astudillo-Salinas, L. Tello-Oquendo, F. Sanchez, G. Lopez, and D. Quiroz, "Information Security Management Frameworks in Higher Education Institutions: An Overview," in 2019 3rd Cyber Security in Networking Conference (CSNet), IEEE, Oct. 2019, pp. 63–65. doi: 10.1109/CSNet47905.2019.9108845.

[85] H. Rehman, A. Masood, and A. R. Cheema, "Information Security Management in Academic Institutes of Pakistan," in 2nd National Conference on Information Assurance (NCIA), 2013, pp. 47–51.

[86] Y. Salem, M. Moreb, and K. S. Rabayah, "Evaluation of Information Security Awareness among Palestinian Learners," in 2021 International Conference on Information Technology (ICIT), IEEE, Jul. 2021, pp. 21–26. doi: 10.1109/ICIT52682.2021.9491639.

[87] N. Taha and L. Dahabiyeh, "College students information security awareness: a comparison between smartphones and computers," Educ Inf Technol (Dordr), vol. 26, no. 2, pp. 1721–1736, Mar. 2021, doi: 10.1007/s10639-020-10330-0.

[88] B. Setiawan and M. A. Rizal, "Measurement of Information Security and Privacy Awareness in College Students after the Covid-19 Pandemic," *Procedia Comput Sci*, vol. 234, pp. 1396–1403, 2024, doi: 10.1016/j.procs.2024.03.138.