Information Security in Higher Education Institutions: A Systematic Literature Review

Bwiino Keefa[1], Geoffrey Kituyi Mayoka[2], Lawrence Nkamwesiga[3] and Makafui Nyamadi[4]

Abstract

Information security in institutions of higher learning continues to be a concern. This is substantiated by the many security-related incidents that have occurred in these institutions over the past decade. In this study, we expound on the vulnerabilities and threats faced by higher education institutions and identify the information security measures that can be adopted to ensure safety. The study identifies insiders, poorly implemented information security frameworks, decentralized networks, Bring Your Own Device (BYOD), and a lack of investment in information security in HEI as the highest vulnerabilities. Accordingly, the study identifies social engineering attacks, distributed denial of service attacks, malware, and insider threats as potential threats and attacks on information in HEI. Furthermore, the findings of this study suggest multi-faceted information security measures encompassing technological, organizational, environmental, and human measures to ensure information security protection in HEI. The study identifies gaps for areas of further research.

Keywords: Information Security, Information Security Measures, Information Security Behavior, Higher Education Institutions, Vulnerabilities, Threats, Risk

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 (Nurse, 2021). 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 extensive and universal access to computer resources (Forrester Research, 2021). Furthermore, it is important to note that the accelerated technological advancements of the Fourth Industrial Revolution have profoundly pervaded higher education institutions, necessitating comprehensive response to the digital transformation of all its aspects (Alenezi, 2023). As systems and devices become increasingly interconnected and perform a wider range of functions, the vulnerability to information security weaknesses as well increases (Do et al., 2018; Nguyen, 2024). 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 (Grama & Milford, 2019) . 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

[1] Makerere University Business School
Email: kbwiino@mubs.ac.ug
[2] Makerere University Business School
[3] Muni University
[4] ICT University

teaching, learning, and research (Li et al., 2023). 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 (De Kock & Futcher, 2016; Li et al., 2023; Moletsane & Tsibolane, 2020). 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 (Cavusoglu, 2004; Edward, 2024; Ulven & Wangen, 2021). According to the Africa Cyber Security Report (2023), the financial impact of cybercrime is projected to escalate, with global losses estimated to reach USD 8 trillion by 2024 and potentially surpass USD 10.5 trillion by 2025. 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 (Bongiovanni, 2019; De Kock & Futcher, 2016; Moletsane & Tsibolane, 2020; Muhenda, 2018).

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 (Moletsane & Tsibolane, 2020). 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., 2022). 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 by Ahmed and Abas (2024) focused on the factors influencing information security policy compliance behavior in higher education institutions ignoring other information security practices.

Extant literature shows that higher education institutions have compelling reasons to investigate information security management (Bongiovanni, 2019; Imbaquingo-Esparza et al., 2022). 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 (Bongiovanni, 2019). 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 (Dioubate et al., 2022; Hina & Dominic, 2017), 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 are the information security vulnerabilities, threats, and attacks faced by higher education institutions?

RQ2. What are the information security measures that can be implemented by higher education institutions to mitigate information security breaches?

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 behaviours, as well as assist researchers in advancing the body of knowledge on information security in these organizational settings.

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 (Dekkers et al., 2022; Snyder, 2019). Second, the retrieved articles are analyzed using predefined criteria to extract the key themes, knowledge gaps, and future research directions.

Literature Search Process

This study employed the structured approach outlined by Xiao and Watson (2019) to provide a comprehensive overview of information security practices in higher education institutions. Rigorous literature search guidelines suggested by Snyder (2019) and Xiao and Watson (2019) 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 (Snyder, 2019). 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 Preferred Reporting Items for Systematic Reviews and Meta-Analyses framework further guided the search process, which ensures a transparent and reproducible methodology.

Filtering Criteria as per the PRISMA

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.

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 (Choong et al., 2014; Wohlin et al., 2022). 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 31 articles that discussed information security practices in higher education institutions. Details are provided in Table 1.

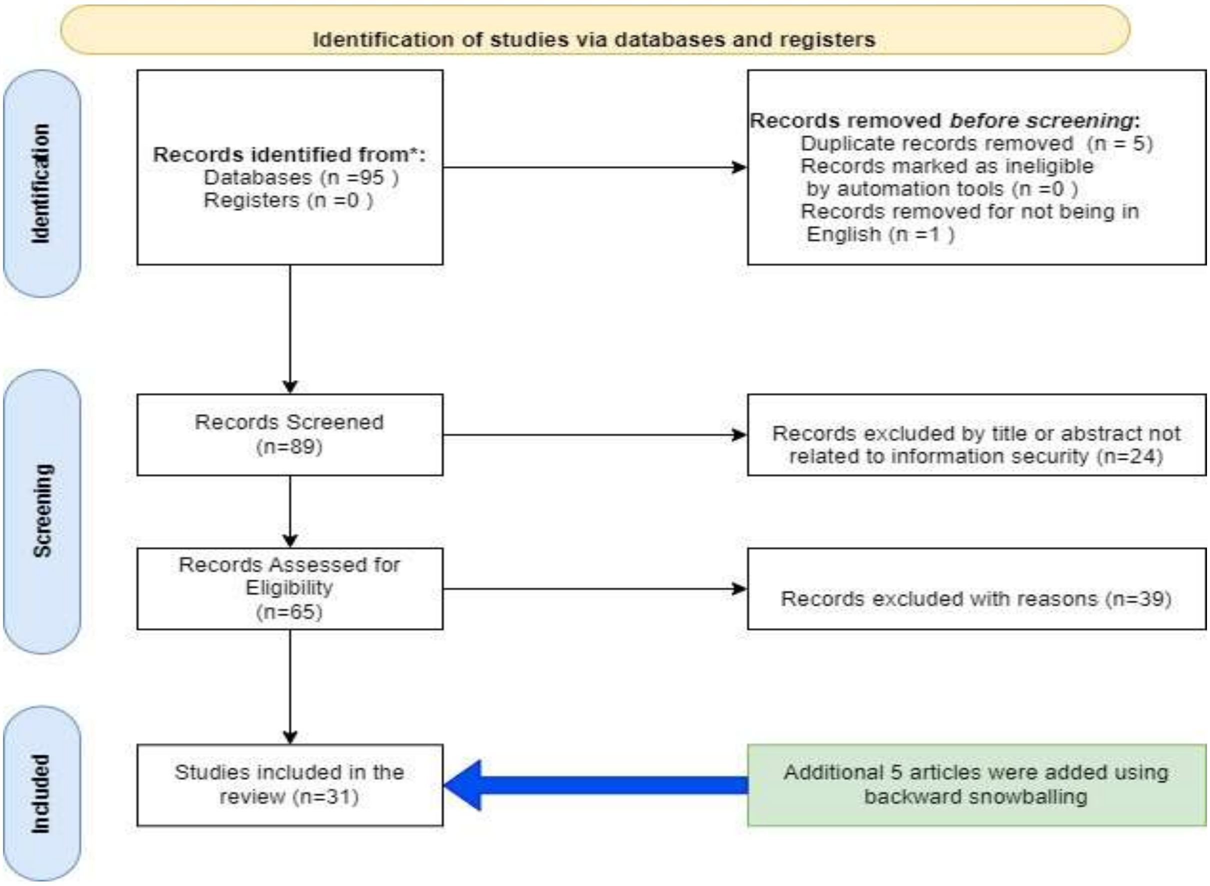
Identification of studies via databases and registers
Identification
Records identified from*:
Databases (n =95)
Registers (n =0)
Records removed before screening:
Duplicate records removed (n = 5)
Records marked as ineligible by automation tools (n =0)
Records removed for not being in English (n =1)
Screening
Records Screened (n=89)
Records excluded by title or abstract not related to information security (n=24)
Records Assessed for Eligibility (n=65)
Records excluded with reasons (n=39)
Included
Studies included in the review (n=31)
Additional 5 articles were added using backward snowballing

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

S/N	Author(s)	Title	Source	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	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	2018	US	Quantitative	Empirical
3	Arina, A., & Anatolie, A	Cyber Security Threat Analysis in Higher Education Institutions as A Result of Distance Learning	*International Journal of Scientific & Technology Research*	2021	US	Qualitative	Conceptual
4	Aborujilah, 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
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	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	2015	Indonesia	Quantitative	Empirical
7	Al-Ibrahim, M., & Shams Al-Deen, Y.	*The Reality of Applying Security in Web Applications in Education*	IEEE Xplore	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	2023	Mexico	Qualitative	Conceptual
9	Daneshmandnia, A.	Exploring Information Security Processes Effectiveness in Educational Institutions: Impacts of Organizational Factors	IEEE Xplore	2023	US	Quantitative	Empirical
10	Flores, P., Farid, M., & Samara, K.	*Assessing E-Security Behavior among Students in Higher Education.*	IEEE Xplore	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	2020		Qualitative	Conceptual
12	Hina, S., & Dominic, D. D.	*Need for Information Security Policies Compliance: A Perspective in Higher Education Institutions*	IEEE Xplore	2017	Malaysia	Quantitative	Empirical
13	Hina, S., & Dominic, D. D.	*Information Security Policies: Investigation of Compliance in Universities*	IEEE Xplore	2016	Malaysia	Quantitative	Empirical

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*	ScienceDirect	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	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.*	ScienceDirect	2017	India	Quantitative	Empirical
17	Kam, H., & Katerattanakul, P.	*Information Security in Higher Education: A Neo-Institutional Perspective*	Taylor and Francis Online	2014	US	Quantitative	Empirical
18	Karabatak, S., & Karabatak, M.	*Information Security Awareness of School Administrators*	IEEE Xplore	2019	Turkey	Quantitative	Empirical
19	RUSERE, K., & NGASSAM, E, K.	*Emerging Network Security Issues in Modern Tertiary Institutions*	IEEE Xplore	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	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	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	Science Direct	2024	Philippines	Quantitative	Empirical
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	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	2019	Malaysia	Quantitative	Empirical
25	Rehman, H., Masood, A., & Cheema, A. R	Information Security Management in Academic Institutes of Pakistan	IEEE Xplore	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	2023	Finland, Malaysia, Thailand	Qualitative	Conceptual

27	Salem, Y., Moreb, M., & Rabayah, K. S.	Evaluation of Information Security Awareness among Palestinian Learners	IEEE Xplore	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	ScienceDirect	2024	Indonesia	Mixed Methods	Empirical
29	Taha, N., & Dahabiyeh, L.	College students information security awareness: a comparison between smartphones and computers.	Springer	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	2023		Qualitative	Conceptual
31	Kam, H.-J., & Katerattanakul, P.	Information Security in Higher Education: A Neo-Institutional Perspective	Taylor and Francis Online	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	2022	Malaysia	Qualitative	Conceptual

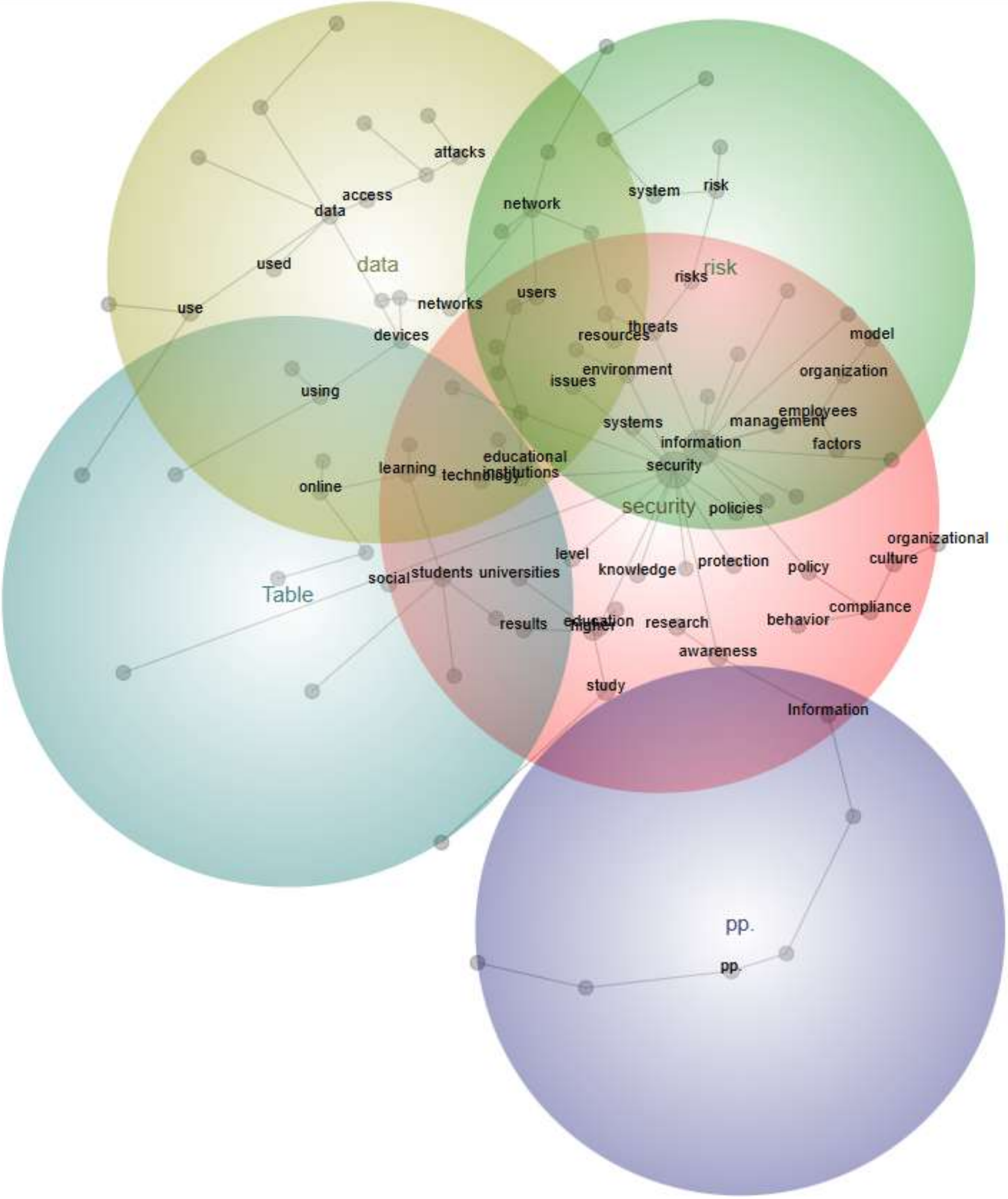

Figure 2: *Concept Map Created using Leximancer*
Source: Author's creation

As illustrated in Figure 2, the concept map synthesizes the key areas of focus examined by researchers in the domain of information security practices within higher education institutions, utilizing the Leximancer analysis tool. The visual inspection of Figure 2 and the findings from the review indicate that the primary theme highlights the challenges higher education institutions face in managing information security and the possible information security measures. The studies emphasize the need for a comprehensive approach to information security, which encompasses technological, organizational, and environmental measures.

Information Security Vulnerabilities, Threats, and Attacks Faced by Higher Education Institutions

Vulnerabilities

This study has identified the following information security vulnerabilities faced by higher education institutions as discussed below:

Firstly, the review has established that factors such as the decentralized nature of higher education institutions, the diverse user base, and the complex information technology infrastructure have contributed to the heightened vulnerability of higher education institutions to cyber threats (Li et al., 2023). These interconnections between many users and different networks make it difficult to centrally control the IT systems used by higher education institutions which allows attackers to exploit higher education institutions. Second, ineffective implementation of cybersecurity risk management frameworks and alignment with international information security standards (Bondoc & Malawit, 2020; Dioubate et al., 2022) is another vulnerability that has enabled information security breaches in higher education institutions as attackers find ways of penetrating poorly implemented information security frameworks (Bondoc & Malawit, 2020).

Accordingly, this study established that insufficient investment in information security measures, including outdated software, inadequate backup systems, and lack of employee training on security best practices (Dioubate et al., 2022; Li et al., 2023) is another area that makes the information security systems of higher education institutions exposed to information security breaches. Academic institutions have been found to have inadequately secured their web applications, leaving them vulnerable to various issues (Al-Ibrahim & Shams Al-Deen, 2014; bin Md Ajis et al., 2020). These include informational problems like broken links, which suggest previously accessible webpages are now inaccessible, email exposure leading to unwanted solicitation, and the storage of user passwords in web browsers. Additionally, there are other 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, slow HTTP denial-of-service attacks, and cross-site scripting (Al-Ibrahim & Shams Al-Deen, 2014).

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 (Ahlan et al., 2015; Alshare et al., 2018; Arina & Anatolie, 2021; Hina & Dominic, 2016; Karabatak & Karabatak, 2019). 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 (Alshare et al., 2018; Arina & Anatolie, 2021).

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 (Canada-Meza et al., 2023). This review has identified the following threats affecting higher education institutions;

Social Engineering Attacks:
Spoofing/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 (Canada-Meza et al., 2023; Rastenis et al., 2019; Rohan et al., 2023). 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 (Rastenis et al., 2019). In some cases, student and staff personal data is being monetized on the black market to further enable these illicit activities.

Insider Threats,
Complacent behavior of stakeholders and unauthorized manipulation or tampering of data poses a significant challenge for higher education institutions (Rohan et al., 2023). Malicious insiders may illicitly access and alter student academic and financial records, leading to data breaches, distortion of institutional records, and financial losses (Canada-Meza et al., 2023; Ganesen et al., 2022; Li et al., 2023). Repudiation which refers to the denial of responsibility by individuals has been recognized as a substantial challenge in higher education institutions (Canada-Meza et al., 2023). Universities frequently struggle to implement effective accountability measures, which can hinder the successful deployment of information security practices. This is a result of failure to identify the users on the network arising from so many connections as well as the Bring Your Own Device (BYOD) mentality that exists in higher education institutions where users modify the institutional security settings on their devices to access unauthorized websites and also connect their devices to unsecured public wireless networks (Moloja et al., 2024; Musarurwa et al., 2017; Rohan et al., 2023). The adoption of Bring-Your-Own-Device practices introduces novel information security challenges for higher education institutions, as personal devices utilized by students and faculty often lack the same robust security safeguards and controls that are typically implemented on institutional-owned equipment (Moloja et al., 2024).

Unauthorized access and misuse of confidential information by university personnel, including the inappropriate escalation of user privileges to restricted systems and data (Canada-Meza et al., 2023; Ganesen et al., 2022; Rohan et al., 2023). 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 (Canada-Meza et al., 2023; Joshi & Singh, 2017).

1. Distributed Denial of Service Attack (DDOS). These attacks seek to overwhelm websites or networks, impairing their performance or rendering them entirely unavailable to users. Higher education institutions are vulnerable to Denial-of-Service attacks, which can lead to resource depletion and system overload, disrupting their operations and services (Bondoc & Malawit, 2020; Canada-Meza et al., 2023).
2. Malware. Higher education institutions also grapple with the threat of ransomware (Bondoc & Malawit, 2020; Flores et al., 2019), which can compromise critical functions and jeopardize the confidentiality of sensitive information.

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 (Aborujilah et al., 2022; Ahlan et al., 2015; Alshare et al., 2018; bin Md Ajis et al., 2020; Hina & Dominic, 2016). This holistic perspective can help identify the most significant determinants for safeguarding critical data assets.

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 (Aborujilah et al., 2022, 2023; bin Md Ajis et al., 2020). 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, (Aborujilah et al., 2023; Arina & Anatolie, 2021; Huerta Suárez et al., 2024). 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 (Toapanta et al., 2023).

Organizational Measures

The literature indicates that higher education institutions can bolster their information security posture through various organizational initiatives (Aborujilah et al., 2022; bin Md Ajis et al., 2020). 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 (Daneshmandnia, 2023; Hina & Dominic, 2020; Liu et al., 2020), implementing security education, training, and awareness programs (SETA) (Arina & Anatolie, 2021; Hina et al., 2019; Hina & Dominic, 2017; Musarurwa et al., 2017; Naga & Tinam-isan, 2024; Ndiege & Okello, 2018; Rohan et al., 2023), developing and enacting information security policies, fostering an information security culture within the institution like enforcement of password policies, adopting risk management practices, separation of personal digital devices from institutional devices (Aborujilah et al., 2023; Ahlan et al., 2015; Alshare et al., 2018; Hina & Dominic, 2020; Joshi & Singh, 2017; Kam & Katerattanakul, 2014; Karabatak & Karabatak, 2019; Rohan et al., 2023), and aligning procedural activities, security initiatives, and the commitment of personnel across all levels, from senior leadership to frontline staff (bin Md Ajis et al., 2020; Karabatak & Karabatak, 2019; Kencana Sari & Nurshabrina, 2016).

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 (bin Md Ajis et al., 2020; Merchan-Lima et al., 2019;

Rehman et al., 2013). Additionally, this review established that external audits are highly influential in information security effectiveness in higher education institutions.

Conclusions

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 (Rohan et al., 2023; Salem et al., 2021; Taha & Dahabiyeh, 2021). 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 (Setiawan & Rizal, 2024; Taha & Dahabiyeh, 2021).

Areas for Future Research

The systematic review has highlighted several promising avenues for future research. These include the need for comparative studies to understand the variations in information security practices across different higher education institutions, a comprehensive examination of the multifaceted factors (human, technological, environmental, and organizational) that influence cybersecurity in the higher education domain, an investigation of information security approaches within distinct academic disciplines, and an exploration of the economic consequences and return on investment associated with information security initiatives in higher education.

References

Aborujilah, A., Adamu, J., Mokhtar, S. A., Al-Othmani, A. Z., Al-alwi, E. Y., & Yahya Al-Hidabi, D. A. (2023). CIA-based Analysis for E-Leaming Systems Threats and Countermeasures in Malaysian Higher Education: Review Paper. *2023 17th International Conference on Ubiquitous Information Management and Communication (IMCOM)*, 1–8. https://doi.org/10.1109/IMCOM56909.2023.10035569

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

Africa Cyber Security Report . (2023).

Ahlan, A. R., Lubis, M., & Lubis, A. R. (2015). Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures. *Procedia Computer Science*, *72*, 361–373. https://doi.org/10.1016/j.procs.2015.12.151

Ahmed, A. A. A., & Abas, H. (2024). Factors Influencing Information Security Policy Compliance Behavior in High Education Institutions: Systematic Literature Review. *Advances in Social Sciences Research Journal*, *11*(7), 260–273.

Alenezi, M. (2023). Digital Learning and Digital Institution in Higher Education. *Education Sciences*, *13*(1), 88. https://doi.org/10.3390/educsci13010088

Al-Ibrahim, M., & Shams Al-Deen, Y. (2014). *The Reality of Applying Security in Web Applications in Education*. www.conference.thesai.org

Alshare, K. A., Lane, P. L., & Lane, M. R. (2018). Information security policy compliance: a higher education case study. *Information & Computer Security*, *26*(1), 91–108. https://doi.org/10.1108/ICS-09-2016-0073

Arina, A., & Anatolie, A. (2021). Cyber Security Threat Analysis In Higher Education Institutions As A Result Of Distance Learning. *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH*, *10*(3), 128–133.

bin Md Ajis, A. F., Rohayu, binti A., & Suhaila, binti O. (2020). *Catalyst of Information Security in Malaysia Higher Learning Institutions*.

Bondoc, C. E., & Malawit, T. G. (2020). Cybersecurity for higher education institutions: adopting regulatory framework. *Global Journal of Engineering and Technology Advances*, *2*(3), 016–021. https://doi.org/10.30574/gjeta.2020.2.3.0013

Bongiovanni, I. (2019). The least secure places in the universe? A systematic literature review on information security management in higher education. *Computers & Security*, *86*, 350–357. https://doi.org/10.1016/j.cose.2019.07.003

Canada-Meza, D. D., Prudente-Tixteco, L., Mercado-Hernandez, P. R., Arenas-Hernandez, J. G., & Ugalde-Eduardo, M. (2023). Recommendations of Security Controls Using Threat Modeling in Information Systems in Higher Education Institutions. *2023 IEEE International Conference on Engineering Veracruz, ICEV 2023*. https://doi.org/10.1109/ICEV59168.2023.10329765

Cavusoglu, H. (2004). Economics of IT Security Management. In *Economics of Information Security* (pp. 71–83). Kluwer Academic Publishers. https://doi.org/10.1007/1-4020-8090-5_6

Choong, M. K., Galgani, F., Dunn, A. G., & Tsafnat, G. (2014). Automatic Evidence Retrieval for Systematic Reviews. *Journal of Medical Internet Research*, *16*(10), e223. https://doi.org/10.2196/jmir.3369

Daneshmandnia, A. (2023). Exploring Information Security Processes Effectiveness in Educational Institutions: Impacts of Organizational Factors). *Proceedings of the 2023 IEEE Asia-Pacific Conference on Computer Science and Data Engineering, CSDE 2023*. https://doi.org/10.1109/CSDE59766.2023.10487771

De Kock, R., & Futcher, L. A. (2016). Mobile device usage in higher education institutions in South Africa. *2016 Information Security for South Africa (ISSA)*, 27–34. https://doi.org/10.1109/ISSA.2016.7802925

Dekkers, R., Carey, L., & Langhorne, P. (2022). Quality of Literature Reviews. In *Making Literature Reviews Work: A Multidisciplinary Guide to Systematic Approaches* (pp. 57–105). Springer International Publishing. https://doi.org/10.1007/978-3-030-90025-0_3

Dioubate, B. M., Daud, W., & Norhayate, W. (2022). Cyber Security Risk Management Frameworks Implementation in Malaysian Higher Education Institutions. *International Journal of Academic Research in Business and Social Sciences*, *12*(4). https://doi.org/10.6007/IJARBSS/v12-i4/12300

Do, C. T., Tran, N. H., Hong, C., Kamhoua, C. A., Kwiat, K. A., Blasch, E., Ren, S., Pissinou, N., & Iyengar, S. S. (2018). Game Theory for Cyber Security and Privacy. *ACM Computing Surveys*, *50*(2), 1–37. https://doi.org/10.1145/3057268

Edward, K. (2024, January 18). *https://www.upguard.com/blog/top-cybersecurity-problems-for-universities-colleges*. Upguard.

Flores, P., Farid, M., & Samara, K. (2019). *Assessing E-Security Behavior among Students in Higher Education*.

Forrester Research. (2021). *Insider Threats Drive Data Protection Improvements Threat Detection, Analytics, And Staffing Lead Investment Priorities*.

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). https://doi.org/10.14569/IJACSA.2022.0130843

Grama, J. L., & Milford, K. (2019). *Ahead of the Curve: IoT Security, Privacy, and Policy in Higher Ed* (pp. 73–86). https://doi.org/10.1007/978-3-030-15705-0_5

Hina, S., & Dominic, D. D. (2016). Information Security Policies: Investigation of Compliance in Universities. *International Conference On Computer And Information Sciences (ICCOINS)*, 564–569.

Hina, S., & Dominic, D. D. (2017). *Need for Information Security Policies Compliance: A Perspective in Higher Education Institutions*. IEEE.

Hina, S., & Dominic, P. D. D. (2020). Information security policies' compliance: a perspective for higher education institutions. In *Journal of Computer Information Systems* (Vol. 60, Issue 3, pp. 201–211). Taylor and Francis Inc. https://doi.org/10.1080/08874417.2018.1432996

Hina, S., Panneer Selvam, D. D. D., & Lowry, P. B. (2019). Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. *Computers & Security*, *87*, 101594. https://doi.org/10.1016/j.cose.2019.101594

Huerta Suárez, C. I., Toapanta T, S. M., Gómez Díaz, E. Z., Huerta Vélez, A. E., Suarez, C. I., & Vizuete, M. Z. (2024). *Analysis for Information Security in Virtual Environments for a Higher Education Institution*. 1739–1745. https://doi.org/10.1109/csci62032.2023.00286

Imbaquingo-Esparza, D., Díaz, J., Ron Egas, M., Fuertes, W., & Molina, D. (2022). *Information Security at Higher Education Institutions: A Systematic Literature Review* (pp. 294–309). https://doi.org/10.1007/978-3-031-18272-3_20

Joshi, C., & Singh, U. K. (2017). Information security risks management framework – A step towards mitigating security risks in university network. *Journal of Information Security and Applications*, *35*, 128–137. https://doi.org/10.1016/j.jisa.2017.06.006

Kam, H.-J., & Katerattanakul, P. (2014). Information Security in Higher Education: A Neo-Institutional Perspective. *Journal of Information Privacy and Security*, *10*(1), 28–43. https://doi.org/10.1080/15536548.2014.912482

Karabatak, S., & Karabatak, M. (2019). *Information Security Awareness of School Administrators* (A. Varol, Ed.). IEEE.

Kencana Sari, P., & Nurshabrina, N. (2016). *Factor Analysis on Information Security Management in Higher Education Institutions*.

Li, J., Xiao, W., & Zhang, C. (2023). Data security crisis in universities: identification of key factors affecting data breach incidents. *Humanities and Social Sciences Communications*, *10*(1), 270. https://doi.org/10.1057/s41599-023-01757-0

Liu, C.-W., Huang, P., & Lucas, H. C. (2020). Centralized IT Decision Making and Cybersecurity Breaches: Evidence from U.S. Higher Education Institutions. *Journal of Management Information Systems*, *37*(3), 758–787. https://doi.org/10.1080/07421222.2020.1790190

Merchan-Lima, J., Astudillo-Salinas, F., Tello-Oquendo, L., Sanchez, F., Lopez, G., & Quiroz, D. (2019). Information Security Management Frameworks in Higher Education Institutions: An Overview. *2019 3rd Cyber Security in Networking Conference (CSNet)*, 63–65. https://doi.org/10.1109/CSNet47905.2019.9108845

Moletsane, T., & Tsibolane, P. (2020). Mobile Information Security Awareness Among Students in Higher Education : An Exploratory Study. *2020 Conference on Information Communications Technology and Society (ICTAS)*, 1–6. https://doi.org/10.1109/ICTAS47918.2020.233978

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

Muhenda, M. B. (2018). *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?*

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

Naga, J. F., & Tinam-isan, M. A. C. (2024). Exploring the influence of personality traits on students' information security risk-taking behaviors: a bfi assessment. *Procedia Computer Science*, *234*, 527–536. https://doi.org/10.1016/j.procs.2024.03.036

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

Nguyen, T. (2024). Understanding Shadow IT usage intention: a view of the dual-factor model. *Online Information Review*, *48*(3), 500–522. https://doi.org/10.1108/OIR-04-2022-0243

Nurse, J. R. C. (2021). Cybersecurity Awareness. In *Encyclopedia of Cryptography, Security and Privacy* (pp. 1–4). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-27739-9_1596-1

Rastenis, J., Ramanauskaitė, S., Janulevičius, J., & Čenys, A. (2019, April 25). Credulity to Phishing Attacks: A Real-World Study of Personnel with Higher Education. *2019 Open Conference of Electrical, Electronic and Information Sciences* .

Rehman, H., Masood, A., & Cheema, A. R. (2013). Information Security Management in Academic Institutes of Pakistan. *2nd National Conference on Information Assurance (NCIA)*, 47–51.

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

Salem, Y., Moreb, M., & Rabayah, K. S. (2021). Evaluation of Information Security Awareness among Palestinian Learners. *2021 International Conference on Information Technology (ICIT)*, 21–26. https://doi.org/10.1109/ICIT52682.2021.9491639

Setiawan, B., & Rizal, M. A. (2024). Measurement of Information Security and Privacy Awareness in College Students after the Covid-19 Pandemic. *Procedia Computer Science*, *234*, 1396–1403. https://doi.org/10.1016/j.procs.2024.03.138

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Taha, N., & Dahabiyeh, L. (2021). College students information security awareness: a comparison between smartphones and computers. *Education and Information Technologies*, *26*(2), 1721–1736. https://doi.org/10.1007/s10639-020-10330-0

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. (2023). Proposal for a security model applying artificial intelligence for administrative management in a higher education institution. *2023 International Conference on Computer, Information and Telecommunication Systems (CITS)*, 1–5. https://doi.org/10.1109/CITS58301.2023.10188801

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

Wohlin, C., Kalinowski, M., Romero Felizardo, K., & Mendes, E. (2022). Successful combination of database search and snowballing for identification of primary studies in systematic literature studies. *Information and Software Technology*, *147*, 106908. https://doi.org/10.1016/j.infsof.2022.106908

Xiao, Y., & Watson, M. (2019). Guidance on Conducting a Systematic Literature Review. *Journal of Planning Education and Research*, *39*(1), 93–112. https://doi.org/10.1177/0739456X17723971