Cybersecurity risks and strategies in learning services of Higher Education Institutions (HEIs) in developing and emerging countries – a critical scoping review

Dr Abdullah Alenezi

Assistant Professor, College of Business Studies, Public Authority for Applied Education and Training, Kuwait

Email: af.alenezi@paaet.edu.kw

Abstract

The adoption of technology in higher education has transformed the landscape of learning services, offering enhanced access and flexibility to students. However, this evolution has introduced new cybersecurity risks, particularly for higher education institutions (HEIs) in developing and emerging countries. This paper adopts a critical scoping review approach to identify published studies on cybersecurity risks and strategies in learning services of HEIs in developing and emerging countries for the period 2014 to 2024. The review highlights the pervasive nature of cybersecurity risks in HEIs, driven by factors such as inadequate resources, outdated systems, and insufficient training. Effective strategies recommended to mitigate these risks include implementing international standards, enhancing cybersecurity education, and developing robust policies. However, significant research gaps remain, particularly regarding the long-term impact of these strategies and the contextual factors of HEIs in these countries. Future research should focus on addressing these gaps, providing a comprehensive understanding of cybersecurity in educational institutions globally.

Keywords: Learning services, cybersecurity risk, higher education institutions, strategies

1. Background

The global landscape of higher education (HE) is undergoing a significant transformation fuelled by the rapid integration of technology. This digital revolution has reshaped learning experiences, offering students enhanced access and flexibility. Higher education institutions (HEIs) are embracing a variety of technological tools, including online platforms like Learning Management Systems (LMS) (Benavides et al., 2020; Veluvali & Surisetti, 2022), Open Educational Resources (OERs) (Berti, 2018), and cloud-based solutions for data storage and access [4]. This shift towards digital learning offers considerable benefits, particularly for students in geographically dispersed regions (UNESCO, 2023). However, this evolution has introduced a new set of cybersecurity challenges, especially for HEIs in emerging countries.

HEIs in emerging countries face a myriad of cybersecurity risks that can compromise the integrity and confidentiality of learning services. One of the primary risks is the susceptibility to cyberattacks due to limited cybersecurity infrastructure and resources (Ulven & Wangen, 2021). These institutions often lack the financial means to invest in robust security measures, making them attractive targets for malicious actors seeking to exploit vulnerabilities. Insufficient awareness among staff and students regarding cybersecurity threats further exacerbates the risks faced by HEIs (Eltahir & Ahmed, 2023; Garba et al.,

2020). Many individuals within these institutions may not fully comprehend the importance of cybersecurity practices or recognize potential threats, increasing the likelihood of successful cyberattacks. Moreover, inadequate infrastructure with outdated or non-existent security features leaves HEIs vulnerable to various cyber threats, including malware, phishing attacks, and data breaches (Maraj et al., 2021; Njoroge et al., 2021). These vulnerabilities make them more susceptible to cyberattacks, potentially risking student data, intellectual property, and disrupting critical learning services. Thus, cybersecurity in learning environments of emerging countries is a critical area of study due to the transformative impact of digitalization on higher education and the specific challenges faced by institutions in these regions. Some examples of recent cyber attacks on HEIs in developing countries are shown in table 1 below:

Table 1: Examples of recent cyber attacks on HEI in developing countries

Institution	**Country**	**Date**
Tshwane University of Technology	South Africa	January 2024
University of Buenos Aires	Argentina	December 2023
De La Salle University	Philippines	October 2023
Universidade Federal de Mato Grosso do Sul	Brazil	September 2023

Safeguarding sensitive student data and maintaining academic records' integrity are crucial aspects of ensuring cybersecurity in learning environments (Ulven & Wangen, 2021). Cyberattacks targeting educational institutions can disrupt critical learning services, leading to downtime and loss of instructional materials, significantly impacting students' academic experiences and outcomes (Merchan-Lima et al., 2021; Mizrak, 2023). Moreover, effective cybersecurity management in learning environments promotes trust in online education systems and facilitates global knowledge exchange, essential for socio-economic development (UNESCO, 2023; Veluvali & Surisetti, 2022). It also plays a vital role in advancing digital inclusion and ensuring equitable access to education, addressing disparities among students from underserved communities (UNESCO, 2023).

Understanding the evolving cyber threat landscape is crucial for developing effective cybersecurity strategies tailored to the unique needs of educational stakeholders in emerging countries (Maranga & Nelson, 2019; Mtakati & Sengati, 2021; Njoroge et al., 2021). Collaborative efforts involving government agencies, educational institutions, industry stakeholders, and international organizations are essential for implementing robust cybersecurity frameworks and regulations (Bondoc & Malawit, 2020; Fouad, 2021). Furthermore, research in cybersecurity for learning environments informs capacity-building initiatives and cybersecurity awareness programs targeted at educators, administrators, and students (Maranga & Nelson, 2019; Triplett, 2023). Therefore, studying cybersecurity in the educational contexts of emerging countries is crucial to address the specific challenges and vulnerabilities faced by these institutions in the digital age. It highlights the need for comprehensive cybersecurity strategies, enhanced collaboration, and the promotion of digital trust to ensure the integrity and accessibility of education for all.

1.1 Aim and objectives

This critical scoping review aims to explore the current state of knowledge on cybersecurity risks and mitigation strategies within the learning services of HEIs in developing and emerging countries. The objectives are to:

- Map the existing literature on cybersecurity risks and strategies in learning services of HEIs in developing and emerging countries.

- Identify the prevalence of cyberattacks targeting online learning platforms and educational resources in developing and emerging countries.
- Analyze the key factors contributing to cybersecurity vulnerabilities in these contexts.
- Identify gaps in the current knowledge base and propose areas for future research.

The primary outcome of this paper is to provide an overview of cybersecurity risks in learning services, the factors contributing to cybersecurity vulnerabilities, and strategies for mitigating these vulnerabilities in higher education institutions (HEIs) in emerging countries. The article also addresses knowledge gaps and suggests future research directions. It is intended for both academics investigating cybersecurity and practitioners actively involved in security within HEIs.

1.2 Definitions

Cybersecurity risk in learning environments refers to the potential threats and vulnerabilities faced by educational institutions, particularly in online and digital learning settings, which can compromise the security and integrity of data, systems, and services (Veluvali & Surisetti, 2022). These risks encompass various cyber threats and attacks that target educational resources, student information, intellectual property, and the overall functioning of learning platforms (Ulven & Wangen, 2021; Veluvali & Surisetti, 2022). The common cybersecurity risks in learning environments include data breaches, malware attacks, phishing, denial-of-service (DoS) attacks, ransomware and insider threats (Fouad, 2021; Liluashvili, 2021; Triplett, 2023).

The review prioritizes studies that specifically investigate cybersecurity issues within higher education institutions situated in countries classified as “developing” and “emerging” economies according to the World Bank classifications. The World Bank classification is based on four income groups according to gross national income (GNI): low, lower-middle, upper-middle, and high income (World Bank, 2024). The developing and emerging countries are those countries in the low to upper middle-income[1] categories with GNI less than $13,845 (World Bank, 2024). These countries represent economies that are transitioning towards higher levels of development and economic stability (World Bank, 2024).

The remainder of this paper is structured as follows:

- Section 2 describes the methodological approach, highlighting the search strategy, inclusive and exclusive criteria
- Section 3 presents the results from the literature review
- Section 4 discusses the findings, identifying key themes and a critique of the selected articles
- Section 5 presents the gap in the literature and direction for future work
- Section 6 concludes the paper

2. Method

A critical scoping review approach has been selected to effectively address the broad objectives of this study. Scoping reviews offer greater flexibility by accommodating a diverse range of study designs (Arksey & O’Malley, 2005). By mapping and summarizing evidence,

[1] Lower-middle income countries are those with GNI per capita between 1,136 to 4,465, while upper-middle income countries are those with GNI per capita of 4,466-13,845 (World Bank, 2024).

scoping reviews can also inform future research directions and contribute to policy considerations (Peters et al., 2020). In this research, the scoping framework proposed by Arksey & O'Malley (2005) has been adopted. This framework entails identifying the research question, locating pertinent studies, applying inclusion criteria to select relevant studies, and then synthesizing and reporting the findings.

2.1 Search strategy

In conducting this scoping review, a comprehensive search strategy was implemented across prominent academic databases, including Scopus, Web of Science, ERIC, and Google Scholar. The search strategy was designed to capture a broad range of literature related to cybersecurity within the context of higher education institutions (HEIs) in developing and emerging countries, focusing specifically on learning services, online learning platforms, and educational resources.

The search strategy involved combining relevant keywords such as "cybersecurity risk", "cybersecurity strategy", "higher education institutions", "emerging countries", "learning services", "online learning platforms", and "educational resources". These keywords were selected to encompass various aspects of cybersecurity challenges and strategies within the educational landscape of the developing and emerging countries. Boolean operators (AND, OR, NOT) were employed to refine the search queries and ensure the retrieval of r articles. The search string used was:

("cybersecurity risk" OR "cybersecurity strategy") AND ("learning services" OR "online learning platforms") AND ("higher education institutions" OR "HEIs") AND ("emerging countries" OR "developing countries").

To ensure comprehensive coverage of relevant literature in the information technology (IT) and management research domains, this review employed a multifaceted approach. Two highly regarded multidisciplinary databases, Scopus and Web of Science, served as the foundation of the search strategy. These platforms index a vast array of scholarly journals, conference proceedings, and books, providing a robust starting point for literature exploration (Harzing & Alakangas, 2016). Furthermore, to specifically target education-related literature on the intersection of cybersecurity and higher education, the Education Resources Information Center (ERIC) database was incorporated. This inclusion ensured the capture of relevant research focusing on educational contexts.

In addition to these established databases, Google Scholar was utilized to supplement the search. This platform provides access to "grey literature," encompassing conference papers and reports that may not be indexed in traditional databases. By leveraging the strengths of these various databases and employing carefully selected search terms, the aim was to identify a diverse range of empirical studies, reviews, case studies, and conceptual papers. This comprehensive search strategy aimed to illuminate the current state of cybersecurity within the learning environments of developing and emerging countries. The scoping review approach adopted in this study emphasizes inclusivity and comprehensiveness, allowing for the exploration of a diverse range of study designs and methodologies (Arksey & O'Malley, 2005). This approach enables a broader mapping and summarization of evidence pertinent to cybersecurity risks and mitigation strategies within the specified context.

The utilization of rigorous search techniques, including keyword selection, Boolean operators, and database selection, enhances the credibility and robustness of the scoping review process. It ensures that the review encompasses a rich diversity of literature, thereby

offering valuable insights into the current state of knowledge and identifying gaps for future research and policy implications.

2.2 Inclusive criteria

The inclusion criteria detail the basis on which sources were considered for inclusion in the scoping review to address the research objectives (Peters et al., 2020). The inclusion criteria were developed as follows:

- Publication Type: Peer-reviewed journal articles and conference proceedings.
- Focus: Studies specifically addressing cybersecurity risks and strategies in learning services of Higher Education Institutions (HEIs) in developing and emerging countries.
- Relevance: Studies published within the last 10 years (2014-2024) to ensure relevance and currency of information.
- Scope: Research that examines various aspects of cybersecurity in learning environments, including online learning platforms, educational resources, data protection, and cyber threats relevant to HEIs in developing and emerging countries.

2.3 Exclusion criteria

- Non-peer-reviewed literature such as editorials, opinion pieces, and non-academic publications.
- Studies not directly related to cybersecurity risks or strategies in the context of HEIs or emerging countries.
- Studies published before 2014.
- Literature focused solely on cybersecurity in non-educational settings or in developed countries.

2.4 Data extraction

The process of screening and selecting studies for inclusion involved several systematic steps to ensure the relevance and quality of the literature reviewed. A comprehensive search was conducted across the selected databases using the specified keywords and search terms. The initial phase of the screen process involved reviewing the titles and abstracts of retrieved articles to assess their relevance based on the predefined inclusion criteria. This entailed excluding articles that clearly do not meet the inclusion criteria, such as those focusing on unrelated topics or developed countries. The screening process aimed to efficiently identify potentially relevant studies for further assessment. Following the screening phase, full-text articles of potentially relevant studies were retrieved for detailed assessment. These were transferred to Mendeley referencing software which helped locate duplications across the searched databases.

Each article underwent a thorough evaluation to determine its eligibility for inclusion based on the established criteria. This involved examining the content, methodology, and alignment with the research focus on cybersecurity risks and strategies within learning services of HEIs in developing and emerging countries.

Upon identifying eligible studies, relevant data was extracted, including key findings, methodologies, and conclusions related to cybersecurity risks and strategies in learning services. A quality assessment of the selected studies was conducted to evaluate their methodological rigor, credibility, and contribution to the research objectives. The “Critical Appraisal Skills Programme” (CASP) checklist was employed to assess the quality of the

selected studies. The CASP checklist provides a structured framework for assessing the methodological quality, validity, and relevance of research studies (CASP, 2024). The tool offers specific criteria and prompts to evaluate different aspects of study design, data collection, analysis, and reporting and can be adapted to assess various types of studies, including qualitative, quantitative, and mixed-methods research (CASP, 2024).

Employing the search strategy resulted in 12 relevant articles. The search process is presented using the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) flow diagram in Figure 1 below:

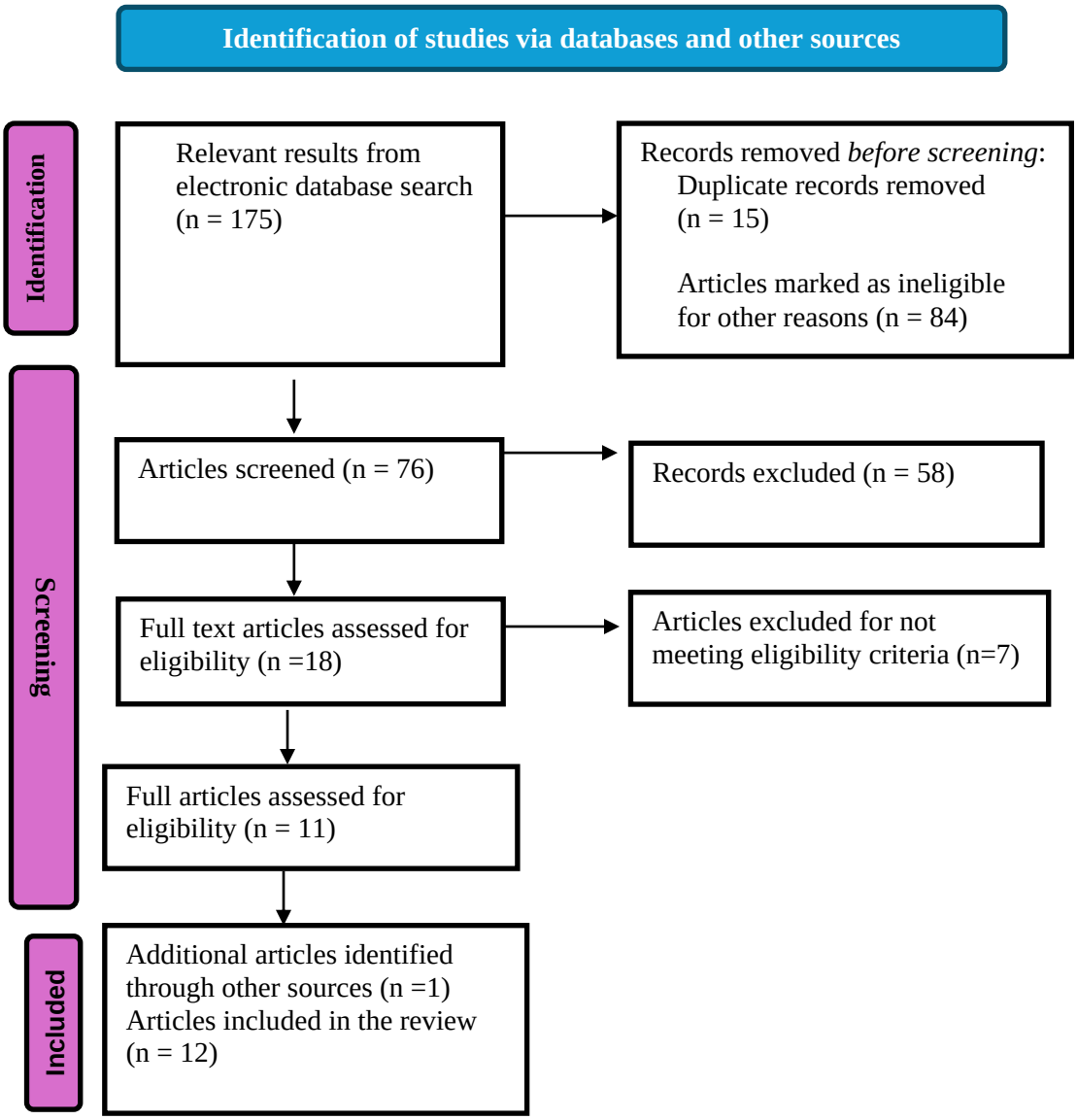

Figure 1: PRISMA flow chart showing the articles identified for critical review.

3. Results

Table 1 below summarises the relevant studies on cybersecurity risk and strategies in learning services of HEIs in developing and emerging countries, satisfying the selection criteria developed following Arksey & O'Malley's framework. There were five empirical papers, three of which involved interviews and two a questionnaire. Most of the papers involved secondary data, reviewing existing literature, assessing the application of a framework or the development of a framework. The author's critical reflections on the findings are discussed in the context of existing body of knowledge.

Table 2: Published articles on cybersecurity risk and strategies in HEI in emerging countries

Author/s (year)	Title	Aim	Country of focus	Theme examined	Method used	Participants	Findings	Strength	Weakness
Amine, A. M., Chakir, E. M., Issam, T., & Khamlichi, Y. I. (2023).	A Review of Cybersecurity Management Standards Applied in Higher Education Institutions	Effective strategies for reinforcing information security within HEIs, amidst the rapidly evolving landscape of information technology and the sophisticated tactics of cyber adversaries	Morocco	Assessment of the ISO/IEC 27001 and NIST Cybersecurity Framework (CSF) standards, which are extensively implemented by Higher Education Institutions (HEIs) to manage cybersecurity risks	Review of literature	N/A	1. Conventional reliance on ISO/IEC 27001 as a recognized standard demands scrutiny, revealing the necessity for tailoring to organizational specifics. 2. NIST-CSF emerges as a robust framework, designed to intricately weave with ISO/IEC 27001, offering HEIs the flexibility to forge bespoke cybersecurity strategies attuned to their distinctive requirements	1. Comparative Analysis: Provides a thorough assessment of ISO/IEC 27001 and NIST-CSF standards, offering insights into their application in HEIs. 2. Customization Insights: Highlights the necessity of tailoring these standards to the specific needs of HEIs, which is a practical consideration.	1. Lack of Empirical Data: The review is based on existing literature without presenting new empirical data or case studies. 2. General Recommendations: The recommendations, while insightful, are broad and may lack specific actionable steps for HEIs.
De Ramos, N. M., & Esponilla, F. D. (2022).	Cybersecurity program for Philippine higher education institutions: A multiple-case study	Cybersecurity threats and challenges of Selected Philippine State Universities and Colleges in the National Capital Region	Philippine	Threats and challenges of cybersecurity to assess active and proactive approaches to developing a model framework for security resources in	Structured interviews	7 participants	Challenges in cybersecurity are user education, cloud security, information security strategy, and unsecured personal devices	1. Multiple-Case Study: Uses a multiple-case study approach, providing a rich and detailed analysis of cybersecurity challenges in several institutions. 2. Proactive	1. Geographical Limitation: Focuses on the National Capital Region of the Philippines, which might limit the generalizability of the findings to other regions. 2. Interview-Based Data: Relies on structured interviews,

Author/s (year)	Title	Aim	Country of focus	Theme examined	Method used	Participants	Findings	Strength	Weakness
				respective academic institutions.				Approaches: Assesses active and proactive approaches, offering insights into effective cybersecurity strategies.	which might not capture the full complexity of cybersecurity challenges.
Cheng, E. C., & Wang, T. (2022).	Institutional Strategies for Cybersecurity in Higher Education Institutions	Bridge this literature gap and generate institutional cybersecurity strategies for HEI leaders and policy-makers from a system perspective	China	Cybersecurity in Higher Education Institutions	Literature review and desk research	N/A	Cybersecurity strategies include (1) Strengthening Institutional Governance for Cybersecurity; (2) Revisiting Cybersecurity KPIs; (3) Explicating Cybersecurity Policies, Guidelines and Mechanisms; (4) Training and Cybersecurity Awareness Campaigns to Build Cybersecurity Culture; (5) Responding to AI-based Cyber-threats and Harnessing AI to Enhance Cybersecurity; (6) Introduction of New and More Sophisticated Security Measures; (7) Paying Attention to Mobile	1. Holistic Approach: Offers a system perspective for generating cybersecurity strategies, covering various aspects such as governance, KPIs, and AI-based threats. 2. Actionable Strategies: Provides specific strategies that HEI leaders and policymakers can implement.	1. Literature Review Limitation: Relies heavily on literature review and desk research, which might not capture the latest trends or challenges. 2. Cultural Specificity: Focuses on China, which might limit the applicability of the findings to HEIs in other cultural or regulatory environments.

Author/s (year)	Title	Aim	Country of focus	Theme examined	Method used	Participants	Findings	Strength	Weakness
							Devices Use, Using Encryption as a Daily Practice; and (8) Risk Management.		
Alexei, L. A., & Alexei, A. (2021).	Cyber Security Threat Analysis In Higher Education Institutions As A Result Of Distance Learning	Identifying the classes of attacks with major impact, on the assets, but also making recommendations for increasing cyber security in e-learning conditions	Moldova	Updating systems and managing security patches, implementing access policies at the application or resource level, classifying information, and using cryptographic protocols	Literature review of academic articles	N/A	Key conclusions of study were: 1) Updating information systems and applications, patch management and automating these processes will ensure a consistent level of is security. 2) To control access to information is very important, so the development of access policies for applications and stored data, mandatory, in order to minimize unauthorized access or compromise of data. Classifying information for restricted access is an important step. 3) The use of secure protocols will allow end users to protect their home network and institutions to protect the	1. Timely Topic: Addresses the relevant issue of cybersecurity threats in the context of distance learning, which has become increasingly important. 2. Comprehensive Recommendations: Offers detailed recommendations for updating systems, managing access, and using cryptographic protocols.	1. Literature Review Limitation: Relies on a literature review, which might not capture the latest developments or empirical data. 2. General Recommendations: The recommendations are broad and might lack specificity for different types of institutions.

Author/s (year)	Title	Aim	Country of focus	Theme examined	Method used	Participants	Findings	Strength	Weakness
							corporate network. The transmitted data will be protected and encrypted. 4) Educating staff and students in the field of information security will reduce the effort of the IT team, and will increase, through distributed efforts, cyber security.		
Alexei, L. A. (2021).	Cyber security strategies for higher education institutions	Identify which is the recommended cyber security strategy and how comprehensive are these studies, within HEIs	Republic of Moldova	Risk management and cyber security strategy, implementation phases, the functions of the security framework, validation methods and the finality of this process.	30 articles	N/A	Study recommends: 1. The creation of a cyber security framework that supports ISO 27001 certification. 2. Building a cyber security framework that will support IT Governance and security policies creation. 3. Risk management is identified as a key activity to implement an effective cyber security strategy.	1. Comprehensive Framework: The article provides a detailed cyber security framework that supports ISO 27001 certification, which is a widely recognized standard in the industry. 2. Risk Management Focus: Emphasizes risk management as a key activity for implementing an effective cyber security strategy, which is crucial	1. Limited Scope: The study is based on 30 articles, which may not fully represent the diverse challenges faced by all HEIs. 2. Geographical Limitation: Focuses primarily on the Republic of Moldova, which might limit the generalizability of the findings to other regions.

Author/s (year)	Title	Aim	Country of focus	Theme examined	Method used	Participants	Findings	Strength	Weakness
								for higher education institutions (HEIs).	
Singar, A.V. and Akhilesh, K. (2020)	Role of Cyber-security in Higher Education	Explores security measures that need to be implemented in the higher education sector	India	Cybersecurity in higher education institutions, including challenges and best practices.	Literature review	N/A	Widespread adoption of Internet of Things (IoT) devices and increased connectivity in HEIs create numerous entry points for potential cyber-attacks. HEI need regular security upgrades	Provides a comprehensive overview of cybersecurity challenges and best practices in higher education.	Lack of empirical data and specific focus on one country's educational institutions, may limit the generalizability of the findings.
Catota, F. E., Morgan, M. G., & Sicker, D. C. (2019).	Cybersecurity education in a developing nation: the Ecuadorian environment	Explores challenges faced by the higher educational system of Ecuador in cybersecurity education and subsequently examines opportunities for improvement.	Ecuador	Cybersecurity education in a developing nation	Qualitative analysis of data	28 semi-structured interviews from thirteen Ecuadorian institutions	Cybersecurity education faces challenges including: cybersecurity skills, structural capabilities, social integration, economic resources, and governance capacity. Solutions include: implement a national cybersecurity education strategy that bolsters multiple initiatives as well as a multi-stakeholder space in which government,	1. Contextual Analysis: Explores the specific challenges and opportunities for cybersecurity education in a developing nation. 2. Diverse Data Sources: Utilizes semi-structured interviews from multiple institutions, providing a rich data set.	1. Regional Focus: The findings are specific to Ecuador, which might limit their applicability to other developing nations. 2. Lack of Solutions: The study identifies challenges but provides limited actionable solutions for overcoming them.

Author/s (year)	Title	Aim	Country of focus	Theme examined	Method used	Participants	Findings	Strength	Weakness
							industry, and academia can actively work together to address national cybersecurity educational requirements.		
Kwaa-Aidoo, E. K., & Agbeko, M. (2018).	An Analysis of Information System Security of a Ghanaian University	Analyse the information system environment of a public Ghanaian university and discusses the state of information security	Ghana	Examining the level of security awareness within a Ghanaian public University	Survey	180 respondents	Study found that: 1. Respondents viewed confidentiality as the most important information security objective followed by integrity and availability. 2. Experienced malware attacks frequently with very few experiencing unauthorised change of information on systems.	1. Survey-Based Analysis: Uses a survey to gather data from a significant number of respondents, providing a broad view of the security awareness within the university. 2. Clear Findings: Identifies specific security concerns such as frequent malware attacks and the importance of confidentiality.	1. Single Institution Focus: The analysis is limited to one university, which might not reflect the situation in other institutions. 2. Limited Depth: The survey approach might not capture the depth and complexity of the information security issues.
Joshi, C., & Singh, U. K. (2017).	Information security risks management framework – A step towards mitigating security risks in university network	Security threats specifically evolve in University's network, and with consideration of these issues, proposed information	India	Mitigating security risks in university network	Quantitative Information Security Risk Assessment Model	N/A	This paper proposes Quantitative Information Security Risk Assessment Model designed specifically for University computing	1. Targeted Framework: Proposes a Quantitative Information Security Risk Assessment Model designed specifically for	1. Lack of Empirical Validation: The proposed model might benefit from empirical validation through case studies or real-world implementation. 2. Broad Approach:

Author/s (year)	Title	Aim	Country of focus	Theme examined	Method used	Participants	Findings	Strength	Weakness
		security framework for University network environment.					environment, with the consideration of security dangers presents in large open campus network of University	university environments. 2. Comprehensive Coverage: Addresses security risks in large open campus networks, which are common in universities.	The recommendations are broad and might lack specific actionable steps for implementation.
Suwito, M. H., Matsumoto , S., Kawamoto , J., Gollmann, D., & Sakurai, K. (2016).	An analysis of IT Assessment Security Maturity in Higher Education Institution	Importance of IT best practices and how to easily harmonize, implement, and integrate these best practices	Indonesia	Assess the implementatio n of security challenges in an organization	Informatio n security maturity model (ISMM)	N/A	Study found that: 1. The combination between IT management methodology using the COBIT® 4.1 and ISO/IEC 27002 give a more comprehensive results and the most efficient in the preparation of implement features. 2. Assessment decision can be made to contain the features of devoted public organization service providers, especially university.	1. Comprehensive Methodologies: Combines COBIT® 4.1 and ISO/IEC 27002, providing a robust framework for IT security assessment. 2. Practical Application: Offers practical insights into the implementation of IT management methodologies.	1. Outdated References: The reliance on COBIT® 4.1 and ITIL® V3, which have newer versions, might reduce the relevance of the findings. 2. Narrow Focus: The study focuses on a specific HEI in Indonesia, limiting the generalizability of the results.
Yilmaz, R., & Yalman, Y. (2016).	A Comparative Analysis of University Information Systems within	Infrastructure, operation, application, information, policy and	Turkey	Enable the universities to compare their information systems with	Qualitative analysis method using Research .	6 universities	Study found that universities: 1. Provide training for their employees for secure application	1. Comparative Approach: Provides a comparative analysis of	1. Tool Limitation: Uses the Microsoft Security Assessment Tool, which does not cover all aspects of

Author/s (year)	Title	Aim	Country of focus	Theme examined	Method used	Participants	Findings	Strength	Weakness
	the Scope of the Information Security Risks	human-based information security at universities were examined within the scope of the information security standards which are highly required and intended to be available at each university today, and then a comparative analysis was conducted specific to Turkey		the information systems of other universities within the scope of the information security awareness, and to make suggestions in this regard	using Microsoft Security Assessment Tool developed by Microsoft was used as the risk analysis tool		development. 2. The human factor directly affected every stage of the analysis. 3. Documenting and keeping documents updated are the common problems of universities and these problems could be overcome by increasing information security awareness among people	information systems security across different universities, offering a broad perspective. 2. Practical Recommendations: Offers actionable recommendations such as training for secure application development and increasing information security awareness.	information security risks. 2. Documenting Issues: Identifies common problems like document updating but does not provide comprehensive solutions for these issues.
Sahri, Z., Abd Aziz, M. E. S., Zolkefley, K. I., Sadjirin, R., & Raus, M. I. M. (2014).	Implementing IT Security Penetration Testing in Higher Education Institute	This paper proposed an enhanced process flow for web deployment process by implementing IT security penetration testing practices in University Teknologi MARA (UiTM) Pahang, Jengka Campus, as a way to early detection, reduce and prevent the	Malaysian	Implementation of Penetration Testing that can be applied in some of the university's IT infrastructure and services.	Qualitative data analysis which applied action research and interviews that requires researcher to study the existing university's IT	Four (4) interviews	Stydy recommends focusing on vulnerability detection and penetration attempt phases during the pen test process to ensure each of security parameter defined above is free from any vulnerabilities.	1. Practical Implementation: Provides a detailed process flow for web deployment and penetration testing, which can be directly applied by other institutions. 2. Early Detection Emphasis: Focuses on early detection and prevention of security	1. Limited Participant Pool: Based on only four interview sessions, which may not provide a comprehensive view of the challenges and solutions. 2. Context Specific: The study is specific to University Teknologi MARA (UiTM) Pahang Jengka Campus, limiting broader applicability.

Author/s (year)	Title	Aim	Country of focus	Theme examined	Method used	Participants	Findings	Strength	Weakness
		institution's information security and services.			security policy, infrastructure and available services.			vulnerabilities.	
Itradat, A., Sultan, S., Al-Junaidi, M., Qaffaf, R., Mashal, F., & Daas, F. (2014).	Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study	Analyzing the risks that faces HU information systems	Jordan	An evaluation of the information security level at the Jordanian universities has been developed by launching a case study targeting HU	vulnerability assessment and penetration testing	N/A	Study found: 1. Inadequate information security awareness for the organization personnel. 2. Organizations do not adopt an information security management system to control the security process of the information systems. 3. Implementing ISO27001 information security management system ISMS	1. Detailed Case Study: Provides an in-depth case study of Hashemite University, offering practical insights into ISO27001 implementation. 2. Awareness Emphasis: Highlights the importance of information security awareness among organization personnel.	1. Single Case Study Limitation: Focuses on one university, which might limit the generalizability of the findings to other institutions. 2. Lack of Quantitative Data: Relies on qualitative data, which might lack the robustness of quantitative analysis.

4. Findings and discussion

The general observations of the reviewed studies are discussed first followed by the identified key themes and a critique of the studies.

4.1 General observations

The articles cover a broad geographical scope, including countries like the Republic of Moldova, Morocco, China, Indonesia, Malaysia, India, Jordan, Ecuador, Ghana, Turkey, and the Philippines. This diversity highlights the varied cybersecurity landscapes and institutional challenges faced by HEIs in different socio-economic and regulatory environments.

Many of the articles, such as those by Alexei (2021) and Amine et al. (2021), emphasize the importance of adopting international standards like ISO/IEC 27001-Information security, cybersecurity and privacy protection, and National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). These frameworks provide a structured approach to managing cybersecurity risks but require customization to fit the unique needs of HEIs in developing countries (Bondoc & Malawit, 2020).

Another key observation are implementation challenges. The implementation of cybersecurity measures is fraught with challenges, including inadequate funding, lack of skilled personnel, and insufficient awareness among stakeholders. Catota et al. (2021) and Kwaa-Aidoo and Agbeko (2018) highlight these issues, pointing to the need for better integration between academia and industry and enhanced cybersecurity education and awareness.

Effective risk management is emphasised, with studies such as Suwito et al. (2016) and Joshi & Singh (2017) discussing the use of maturity models and risk assessment frameworks. These tools help institutions identify and mitigate potential threats but also require significant resources and expertise to implement effectively. In addition, the practical aspect of cybersecurity is addressed through studies on penetration testing and vulnerability assessments, such as Sahri et al. (2014). These techniques are essential for identifying and addressing security gaps but are often underutilized due to resource constraints.

Cybersecurity education and policy development are critical for building a robust security culture within HEIs. The studies of Cheng & Wang (2022) and De Ramos & Esponilla (2022) highlight the importance of cybersecurity governance, training, and awareness campaigns, suggesting that a proactive approach is necessary for long-term security improvements. Cybersecurity awareness in HEI has been investigated in several other studies, supporting the need for training and awareness campaigns among students and staff (Aljohni et al., 2021; Eltahir & Ahmed, 2023; Garba et al., 2020).

4.2 Key themes

4.2.1 Prevalence of cybersecurity risks in learning services

Cybersecurity risks in higher education are both pervasive and varied, manifesting differently across geographic and technological contexts. Kwaa-Aidoo & Agbeko (2018) highlight a high prevalence of security risks at a Ghanaian university, attributing these issues to inadequate infrastructure and outdated systems. The lack of robust security frameworks and reliance on obsolete technology make these institutions vulnerable to cyberattacks, a situation exacerbated by limited resources and technical constraints typical of developing countries.

Itradat et al. (2014) offer a parallel perspective from Hashemite University, where significant cybersecurity risks such as data breaches and unauthorized access were prevalent before the implementation of the ISO27001 Information Security Management System (ISMS). The absence of formal security protocols and inconsistent security practices across departments contributed to these vulnerabilities. Similarly, Yilmaz & Yalman (2016) identify common security risks like data theft and system vulnerabilities across multiple universities, suggesting that these issues are not isolated to specific regions but are widespread across the higher education sector.

Singar & Akhilesh (2020) add another perspective to this discussion by examining the role of smart technologies in exacerbating cybersecurity threats. The widespread adoption of Internet of Things (IoT) devices and increased connectivity in HEIs create numerous entry points for potential cyber-attacks, highlighting the need for corresponding security upgrades. This notion is echoed by Alexei & Alexei (2021), who discuss the increased cybersecurity risks associated with the shift towards distance learning. The rapid transition to remote education, especially during the COVID-19 pandemic, has not been matched with adequate cybersecurity measures, leaving institutions exposed to various threats.

In the context of cybersecurity programs in Philippine higher education institutions, De Ramos & Esponilla (2022) underscore the frequent cybersecurity incidents and lack of adequate defense mechanisms. These incidents highlight the need for comprehensive cybersecurity strategies and better resource allocation to enhance security. Maraj et al. (2021) and Catota et al. (2019) provide insights from Kosovo and Ecuador respectively, emphasizing the prevalence of cybersecurity risks due to insufficient training, resources, and institutional support. The lack of adequate cybersecurity education and awareness further contribute to the vulnerabilities faced by these institutions.

4.2.2 Contributing factors to cybersecurity vulnerabilities

Several factors contribute to the cybersecurity vulnerabilities in higher education. Kwaa-Aidoo & Agbeko (2018) point out that limited resources, inadequate infrastructure, and a lack of cybersecurity awareness among staff and students are significant issues, particularly in developing countries. These constraints hinder the implementation of robust security measures, leaving institutions vulnerable to cyber threats. Itradat et al. (2014) identify resistance to change, lack of skilled personnel, and inadequate initial security measures as significant factors complicating the implementation of standardized security frameworks like ISO27001 Information Security Management System. The rapid adoption of smart technologies without corresponding security upgrades also contributes significantly to cybersecurity vulnerabilities (Alexei & Alexei, 2021). The integration of IoT devices and smart technologies increases the attack surface, creating more opportunities for cyber-attacks (Singar & Akhilesh, 2020).

Yilmaz & Yalman (2016) emphasize the role of inconsistent security policies, outdated systems, and lack of regular security assessments in contributing to cyber-attack vulnerabilities. The disparity in security practices across different departments within the same institution further exacerbates these issues. De Ramos & Esponilla (2022) highlight insufficient cybersecurity training, limited funding, and inadequate policy frameworks as key factors preventing institutions from developing and maintaining effective cybersecurity defences.

Maraj et al. (2021) and Catota et al. (2019) discuss the significant role of resource constraints and lack of institutional support for cybersecurity education in contributing to vulnerabilities. The absence of a coordinated approach to cybersecurity education leaves

students and staff ill-prepared to handle cyber threats. Alexei & Alexei (2021) also highlight the increased reliance on online platforms and insufficient cybersecurity measures for remote learning as contributing factors, especially during the pandemic-induced shift to online education. Alexei (2021) further points out that weak cybersecurity policies and inadequate funding for cybersecurity initiatives are significant factors, as institutions struggle to prioritize cybersecurity amid competing financial demands.

4.2.3 Strategies for mitigating cybersecurity risks

Several strategies have been proposed to mitigate cybersecurity risks in HEIs. Kwaa-Aidoo & Agbeko (2018) suggest improving infrastructure, increasing cybersecurity awareness, and implementing robust security policies as key strategies. These measures can help mitigate the risks associated with inadequate security frameworks and outdated systems. Itradat et al. (2014) recommend implementing ISO27001 standards, continuous monitoring, and training for staff to ensure that security practices are standardized and that staff are equipped to handle cybersecurity threats.

Singar & Akhilesh (2020) advocate for incorporating cybersecurity into educational curricula, regular security assessments, and leveraging advanced technologies. These approaches help build a security-conscious culture and ensure that institutions keep pace with evolving cyber threats. Yilmaz & Yalman (2016) recommend developing consistent security policies, upgrading systems, and conducting regular training to address the vulnerabilities associated with inconsistent security practices and outdated systems.

De Ramos & Esponilla (2022) suggest establishing comprehensive cybersecurity programs, improving policy frameworks, and increasing funding for cybersecurity initiatives. These measures ensure that institutions have the resources and policies needed to defend against cyber threats. Maraj et al. (2021) and Catota et al. (2019) emphasize enhancing cybersecurity education, fostering international collaborations, and securing additional resources. These approaches help build capacity and ensure that institutions can access the resources needed to improve cybersecurity.

Alexei & Alexei (2021) recommend strengthening security measures for online platforms, conducting regular risk assessments, and training staff and students. These approaches help mitigate the risks associated with the increased reliance on online education. Alexei (2021) advocates for formulating and implementing robust cybersecurity policies, securing adequate funding, and enhancing security education to ensure that institutions have the resources and policies needed to defend against cyber threats.

4.3 Critique of the studies

Some key strengths of the studies reviewed include comprehensive coverage, contextual relevance and methodological diversity. The studies collectively cover a wide range of topics related to cybersecurity in HEIs, including strategic frameworks, implementation challenges, risk management, and educational initiatives. This comprehensive coverage provides a somewhat holistic view of the cybersecurity landscape in developing and emerging countries. Further, by focusing on specific countries and regions, the articles offer insights that are highly relevant to the local context. This approach helps identify region-specific challenges and tailor solutions that are more likely to be effective. The review also highlights the methodological diversity including literature reviews, case studies, surveys, and qualitative analyses, which enriches the findings and provides multiple perspectives on the issue of cybersecurity in HEIs.

However, there are notable limitations related to limited generalisability, reliance on secondary data, resource constraints and broad recommendations. The regional focus, while

providing contextual relevance, also limits the generalizability of the findings. The specific challenges and solutions identified in one country may not be applicable to others with different socio-economic and regulatory environments. Further, most studies (Alexei, 2021; Alexei & Alexei, 2021; Cheng & Wang, 2022) rely heavily on literature reviews and secondary data, which may not capture the latest trends or empirical realities. Primary data collection through surveys and interviews, as seen in some studies (Kwaa-Aidoo & Agbeko, 2018; Catota et al., 2021), could provide more current and actionable insights.

Most studies (De Ramos & Esponilla, 2022; Kwaa-Aidoo & Agbeko, 2018; Itradat et al., 2014; Yilmaz & Yalman, 2016) highlight the lack of resources, both financial and human, as a significant barrier to implementing effective cybersecurity measures. However, few offer detailed strategies for overcoming these constraints, which is a critical gap in the research. In addition, some studies (De Ramos & Esponilla, 2022) provide broad recommendations without specific, actionable steps. For example, while emphasizing the need for cybersecurity education and awareness is important, detailed curricula and implementation plans would be more beneficial.

5. Gaps in knowledge and future research direction

Despite the extensive research on cybersecurity in higher education, significant gaps remain. Kwaa-Aidoo & Agbeko (2018) identify a lack of research on the specific challenges faced by African universities. Future studies should investigate region-specific cybersecurity solutions and their effectiveness in addressing the unique challenges of developing countries. Itradat et al. (2014) highlight the need for longitudinal studies to assess the long-term impact of ISO27001 implementation. Future research should explore the adaptation of ISO27001 in different educational contexts to identify best practices and potential challenges.

Singar & Akhilesh (2020) point out a lack of comprehensive studies on the integration of smart technologies and cybersecurity. Future research should evaluate the effectiveness of smart technology security measures in education to ensure that institutions can leverage these technologies safely. Yilmaz & Yalman (2016) identify insufficient comparative studies across diverse educational institutions. Broader comparative analyses should be conducted to identify best practices and common challenges across different types of institutions.

De Ramos & Esponilla (2022) highlight the limited number of case studies on cybersecurity programs in developing countries. Future research should expand case studies to include more institutions and regions to provide a comprehensive understanding of the challenges and solutions in different contexts. Maraj et al. (2021) emphasize the need for research on the scalability of cybersecurity education programs. Future studies should investigate scalable models for cybersecurity education in resource-constrained environments to ensure that all institutions can access effective training.

Catota et al. (2019) identify a lack of studies on the impact of cybersecurity training on actual security outcomes. Future research should assess the effectiveness of different training methodologies to identify the most effective approaches to cybersecurity education. Alexei & Alexei (2021) highlight limited research on cybersecurity challenges specific to distance learning. Future studies should explore targeted cybersecurity strategies for online education platforms to address the unique risks associated with remote learning. Alexei (2021) points out insufficient data on the long-term impact of cybersecurity policies in education. Longitudinal studies could be conducted to evaluate the effectiveness of cybersecurity policies over time to ensure that they provide lasting protection.

6. Conclusion

The reviewed articles collectively highlight the pervasive nature of cybersecurity risks in higher education, driven by factors such as inadequate resources, outdated systems, and insufficient training. Effective strategies to mitigate these risks include implementing international standards, enhancing cybersecurity education, and developing robust policies. However, significant gaps remain, particularly regarding the long-term impact of these strategies and the specific challenges faced by developing countries. Future research should focus on addressing these gaps, providing a comprehensive understanding of cybersecurity in educational institutions globally.

The prevalence of cybersecurity risks in higher education is a significant concern. Institutions are increasingly reliant on digital technologies, making them attractive targets for cyber-attacks. The studies revealed that inadequate infrastructure, insufficient cybersecurity measures, and the rapid adoption of smart technologies without corresponding security upgrades are major contributing factors to these risks. Additionally, inconsistent security policies, outdated systems, and lack of regular security assessments further exacerbate vulnerabilities.

To mitigate these risks, various strategies have been proposed. These include improving infrastructure, increasing cybersecurity awareness, and implementing robust security policies. Additionally, the implementation of international standards such as ISO27001, continuous monitoring, and staff training are crucial. Incorporating cybersecurity into educational curricula, regular security assessments, and leveraging advanced technologies are also recommended. Furthermore, developing consistent security policies, upgrading systems, and conducting regular training can help address vulnerabilities.

Despite these strategies, significant gaps remain in knowledge and research. There is a need for more studies on the specific challenges faced by educational institutions in different regions, particularly in developing and emerging countries. Future research should focus on region-specific cybersecurity solutions, the long-term impact of implementing international standards, and the effectiveness of smart technology security measures. Comparative studies across diverse educational institutions, case studies on cybersecurity programs in developing and emerging countries, and research on scalable cybersecurity education models are also needed. Additionally, assessing the impact of cybersecurity training on actual security outcomes and exploring targeted strategies for online education platforms are important areas for future research.

In conclusion, while significant progress has been made in understanding and addressing cybersecurity risks in higher education, there is still much to be done. Institutions must continue to prioritize cybersecurity, implement effective strategies, and stay abreast of evolving threats. Through continued research and collaboration, we can develop a comprehensive understanding of cybersecurity in educational institutions and ensure that they are equipped to handle the challenges of the digital age.

It’s also important to acknowledge that while this review has addressed its objectives on the cybersecurity issues in HEIs in developing and emerging countries, the vastness of the subject means that not all aspects have been thoroughly examined. Consequently, some important topics may be underrepresented, and the review might not fully capture the complexity of cybersecurity challenges in different contexts.

References

Alexei, L.A., 2021. Cyber security strategies for higher education institutions. Journal of Engineering Sciences, (4), pp.74-92. Doi.org/10.52326/jes.utm.2021.28(4).07

Alexei, L.A. and Alexei, A., 2021. Cyber security threat analysis in higher education institutions as a result of distance learning. International Journal of Scientific and Technology Research, (3), pp.128-133.

Aljohni, W., Elfadil, N., Jarajreh, M. and Gasmelsied, M., 2021. Cybersecurity awareness level: The case of Saudi Arabia university students. International Journal of Advanced Computer Science and Applications, 12(3), pp.276-281. Doi.org/10.14569/ijacsa.2021.0120334

Amine, A.M., Chakir, E.M., Issam, T. and Khamlichi, Y.I., 2023. A review of cybersecurity management standards applied in higher education institutions. International Journal of Safety & Security Engineering, 13(6). Doi.org/10.18280/ijsse.130614

Arksey, H. and O'Malley, L., 2005. Scoping studies: towards a methodological framework. International Journal of Social Research Methodology, 8(1), pp.19-32. Doi.org/10.1080/1364557032000119616

Benavides, L.M.C., Tamayo Arias, J.A., Arango Serna, M.D., Branch Bedoya, J.W. and Burgos, D., 2020. Digital transformation in higher education institutions: A systematic literature review. Sensors, 20(11), p.3291. Doi.org/10.3390/s20113291

Berti, M., 2018. Open educational resources in higher education. Issues and Trends in Learning Technologies, 6(1). Doi.org/10.2458/azu_itet_v6i1_berti

Bondoc, C.E. and Malawit, T.G., 2020. Cybersecurity for higher education institutions: Adopting regulatory framework. Global Journal of Engineering and Technology Advances, 2(3), pp.016-021. Doi.org/10.30574/gjeta.2020.2.3.0013

Catota, F.E., Morgan, M.G. and Sicker, D.C., 2019. Cybersecurity education in a developing nation: The Ecuadorian environment. Journal of Cybersecurity, 5(1), p.tyz001. Doi.org/10.1093/cybsec/tyz001

Cheng, E.C. and Wang, T., 2022. Institutional strategies for cybersecurity in higher education institutions. Information, 13(4), p.192. Doi.org/10.3390/info13040192

Critical Appraisal Skills Programme (CASP). CASP checklist [Internet]. Available at: https://casp-uk.net/casp-tools-checklists/ [Accessed 01/07/2024].

De Ramos, N.M. and II, F.D.E., 2022. Cybersecurity program for Philippine higher education institutions: A multiple-case study. International Journal of Evaluation & Research in Education, 2252(8822), p.1199. Doi.org/10.11591/ijere.v11i3.22863

Eltahir, M.E. and Ahmed, O.S., 2023. Cybersecurity awareness in African higher education institutions: A case study of Sudan. Inf. Sci. Lett., 12(1), pp.171-183. Doi.org/10.18576/isl/120113

Fouad, N.S., 2021. Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. Journal of Cyber Policy, 6(2), pp.137-154. Doi.org/10.1080/23738871.2021.1973526

Garba, A., Sirat, M.B., Hajar, S. and Dauda, I.B., 2020. Cyber security awareness among university students: A case study. Science Proceedings Series, 2(1), pp.82-86. Doi.org/10.31580/sps.v2i1.1320

Harzing, A.W. and Alakangas, S., 2016. Google Scholar, Scopus and the Web of Science: a longitudinal and cross-disciplinary comparison. Scientometrics, 106, pp.787-804. Doi.org/10.1007/s11192-015-1798-9

Itradat, A., Sultan, S., Al-Junaidi, M., Qaffaf, R., Mashal, F. and Daas, F., 2014. Developing an ISO27001 information security management system for an educational institute: Hashemite University as a case study. Jordan Journal of Mechanical and Industrial Engineering, 8, pp.102-118.

Joshi, C. and 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, pp.128-137. Doi.org/10.1016/j.jisa.2017.06.006

Kwaa-Aidoo, E.K. and Agbeko, M., 2018. An analysis of information system security of a Ghanaian university. International Journal of Information Security Science, 7, pp.90-99.

Liluashvili, G.B., 2021. Cyber risk mitigation in higher education. Law & World, 17, p.15. Doi.org/10.36475/7.2.2

Maraj, A., Sutherland, C. and Butler, W., 2021, June. The challenges to cybersecurity education in developing countries: A case study of Kosovo. In ECCWS 2021 20th European Conference on Cyber Warfare and Security (p. 260). Academic Conferences Inter Ltd. Doi.org/10.34190/ews.21.003

Maranga, M.J. and Nelson, M., 2019. Emerging issues in cyber security for institutions of higher education. International Journal of Computer Science and Network, 8(4), pp.371-379.

Merchan-Lima, J., Astudillo-Salinas, F., Tello-Oquendo, L., Sanchez, F., Lopez-Fonseca, G. and Quiroz, D., 2021. Information security management frameworks and strategies in higher education institutions: A systematic review. Annals of Telecommunications, 76, pp.255-270. Doi.org/10.1007/s12243-020-00783-2

Mızrak, F., 2023. Integrating cybersecurity risk management into strategic management: a comprehensive literature review. Research Journal of Business and Management, 10(3), pp.98-110. Doi.org/10.17261/pressacademia.2023.1807

Mtakati, B. and Sengati, F., 2021. Cybersecurity posture of higher learning institutions in Tanzania. The Journal of Informatics, 1(1). Doi.org/10.59645/tji.v1i1.1

Njoroge, P.M., Ogalo, J.O. and Ratemo, C.M., 2021. Information system security practices and implementation issues and challenges in public universities. European Journal of Information Technologies and Computer Science, 1(5), pp.11-15. Doi.org/10.24018/compute.2021.1.5.30

Triplett, W.J., 2023. Addressing cybersecurity challenges in education. International Journal of STEM Education for Sustainability, 3(1), pp.47-67. Doi.org/10.53889/ijses.v3i1.132

Ulven, J.B. and Wangen, G., 2021. A systematic review of cybersecurity risks in higher education. Future Internet, 13(2), p.39. Doi.org/10.3390/fi13020039

UNESCO, 2024. Digital learning and transformation of education (online). Available at: https://www.unesco.org/en/digital-education [Accessed 01/06/2024].

Sahri, Z., Abd Aziz, M.E.S., Zolkefley, K.I., Sadjirin, R. and Raus, M.I.M., 2014. Implementing IT security penetration testing in higher education institute. Australian Journal of Basic and Applied Sciences, 8(21), pp.67-72.

Singar, A.V. and Akhilesh, K., 2020. Role of cyber-security in higher education. In Smart Technologies (pp. 249–264). Springer, Berlin/Heidelberg, Germany. Doi.org/10.1007/978-981-13-7139-4_19

Suwito, M.H., Matsumoto, S., Kawamoto, J., Gollmann, D. and Sakurai, K., 2016. An analysis of IT assessment security maturity in higher education institution. In Information Science and Applications (ICISA) 2016 (pp. 701-713). Springer Singapore. Doi.org/10.1007/978-981-10-0557-2_69

Sych, T., Khrykov, Y. and Ptakhina, O., 2021. Digital transformation as the main condition for the development of modern higher education. Educational Technology Quarterly, 2021(2), pp.293-309. Doi.org/10.55056/etq.27

Veluvali, P. and Surisetti, J., 2022. Learning management system for greater learner engagement in higher education—A review. Higher Education for the Future, 9(1), pp.107-121. Doi.org/10.1177/2347631121104

World Bank, 2024. World Bank Group country classifications by income level for FY24 (July 1, 2023 - June 30, 2024) (online). Available at: https://blogs.worldbank.org/en/opendata/new-world-bank-group-country-classifications-income-level-fy24 [Accessed 10/07/2024].

Yilmaz, R. and Yalman, Y., 2016. A comparative analysis of university information systems within the scope of the information security risks. TEM Journal, 5, pp.180-191.

Appendix

Appendix 1: PRIMA Checklist

Preferred Reporting Items for Systematic reviews and Meta-Analyses extension for Scoping Reviews (PRISMA-ScR) Checklist

SECTION	ITEM	PRISMA-ScR CHECKLIST ITEM	REPORTED ON PAGE #
TITLE			
Title	1	Identify the report as a scoping review.	1
ABSTRACT			
Structured summary	2	Provide a structured summary that includes (as applicable): background, objectives, eligibility criteria, sources of evidence, charting methods, results, and conclusions that relate to the review questions and objectives.	1
INTRODUCTION			
Rationale	3	Describe the rationale for the review in the context of what is already known. Explain why the review questions/objectives lend themselves to a scoping review approach.	1-2
Objectives	4	Provide an explicit statement of the questions and objectives being addressed with reference to their key elements (e.g., population or participants, concepts, and context) or other relevant key elements used to conceptualize the review questions and/or objectives.	2
METHODS			
Protocol and registration	5	Indicate whether a review protocol exists; state if and where it can be accessed (e.g., a Web address); and if available, provide registration information, including the registration number.	N/A
Eligibility criteria	6	Specify characteristics of the sources of evidence used as eligibility criteria (e.g., years considered, language, and publication status), and provide a rationale.	4-5
Information sources*	7	Describe all information sources in the search (e.g., databases with dates of coverage and contact with authors to identify additional sources), as well as the date the most recent search was executed.	4
Search	8	Present the full electronic search strategy for at least 1 database, including any limits used, such that it could be repeated.	3-4
Selection of sources of evidence†	9	State the process for selecting sources of evidence (i.e., screening and eligibility) included in the scoping review.	5
Data charting process‡	10	Describe the methods of charting data from the included sources of evidence (e.g., calibrated forms or forms that have been tested by the team before their use, and whether data charting was done	5-7

SECTION	ITEM	PRISMA-ScR CHECKLIST ITEM	REPORTED ON PAGE #
		independently or in duplicate) and any processes for obtaining and confirming data from investigators.	
Data items	11	List and define all variables for which data were sought and any assumptions and simplifications made.	N/A
Critical appraisal of individual sources of evidence§	12	If done, provide a rationale for conducting a critical appraisal of included sources of evidence; describe the methods used and how this information was used in any data synthesis (if appropriate).	5
Synthesis of results	13	Describe the methods of handling and summarizing the data that were charted.	6-12
RESULTS			
Selection of sources of evidence	14	Give numbers of sources of evidence screened, assessed for eligibility, and included in the review, with reasons for exclusions at each stage, ideally using a flow diagram.	6
Characteristics of sources of evidence	15	For each source of evidence, present characteristics for which data were charted and provide the citations.	6-12
Critical appraisal within sources of evidence	16	If done, present data on critical appraisal of included sources of evidence (see item 12).	8-12, 15
Results of individual sources of evidence	17	For each included source of evidence, present the relevant data that were charted that relate to the review questions and objectives.	6-12
Synthesis of results	18	Summarize and/or present the charting results as they relate to the review questions and objectives.	7-12
DISCUSSION			
Summary of evidence	19	Summarize the main results (including an overview of concepts, themes, and types of evidence available), link to the review questions and objectives, and consider the relevance to key groups.	18
Limitations	20	Discuss the limitations of the scoping review process.	22-23
Conclusions	21	Provide a general interpretation of the results with respect to the review questions and objectives, as well as potential implications and/or next steps.	22-23
FUNDING			
Funding	22	Describe sources of funding for the included sources of evidence, as well as sources of funding for the scoping review. Describe the role of the funders of the scoping review.	N/A

ملخص الدراسة:

لقد أدى تبني التكنولوجيا في التعليم العالي إلى تحويل مشهد خدمات التعليم، مما يوفر وصولاً أفضل ومرونة اعلى للطلبه. ومع ذلك، فقد أدخل هذا التطور العديد من المخاطر الجديدة للأمن السيبراني، وخاصة بالنسبة لمؤسسات التعليم العالي في البلدان النامية والناشئة. تتبنى هذه الورقة نهج المراجعة النقدية لتحدد وتسلط الضوء على الدراسات المنشورة حول مخاطر واستراتيجيات الأمن السيبراني في خدمات التعليم لمؤسسات التعليم العالي في البلدان النامية والناشئة للفترة من ٢٠١٤ إلى ٢٠٢٤. بالإضافة إلى انها تسلط الضوء على الطبيعة الشاملة لمخاطر الأمن السيبراني في مؤسسات التعليم العالي، مدفوعة بعوامل مثل عدم كفاية الموارد، والأنظمة القديمة، والتدريب غير الكافي. تشمل الاستراتيجيات الفعالة الموصى بها للتخفيف من هذه المخاطر تنفيذ المعايير الدولية، وتعزيز تعليم الأمن السيبراني، وتطوير سياسات قوية. ومع ذلك، لا تزال هناك فجوات بحثية كبيرة، وخاصة فيما يتعلق بالتأثير الطويل الأجل لهذه الاستراتيجيات والعوامل المرتبطة بها لمؤسسات التعليم العالي في هذه البلدان. يجب أن تركز الأبحاث المستقبلية على معالجة هذه الفجوات، وتوفير فهم شامل للأمن السيبراني في المؤسسات التعليمية على مستوى العالم.