Online-Journals.org

iJET International Journal of Emerging Technologies in Learning

iJET | eISSN: 1863-0383 | Vol. 18 No. 15 (2023) | OPEN ACCESS

https://doi.org/10.3991/ijet.v18i15.40673

PAPER

ICT Security Tools and Techniques among Higher Education Institutions: A Critical Review

Miko Nuñez[1,2], Xavier-Lewis Palmer[3], Lucas Potter[3], Chris Jordan Aliac[4], Lemuel Clark Velasco[1,5](✉)

[1]Mindanao State University Iligan Institute of Technology, Iligan City, the Philippines

[2]CyTech USA LLC, Denver, Colorado, USA

[3]Old Dominion University, Norfolk, Virginia, USA

[4]Cebu Institute of Technology University, Cebu City, the Philippines

[5]Premiere Research Institute of Science and Mathematics Center for Computational Analytics and Modelling, Iligan City, the Philippines

lemuelclark.velasco@g.msuiit.edu.ph

ABSTRACT

Higher education institutions (HEIs) are increasingly relying on digital technologies for classroom and organizational management, but this puts them at higher risk for information and communication (ICT security attacks. Recent studies show that HEIs have experienced more security breaches in ICT security composed of both cybersecurity an information security. A literature review was conducted to identify common ICT security practices in HEIs over the last decade. 11 journal articles were profiled and analyzed, revealing threats to HEIs' security and protective measures in terms of organizational security, technological security, physical security, and standards and frameworks. Security tools and techniques were grouped into categories with specific ways to protect ICT security. HEIs also implement general security standards and guidelines, such as the ISO 27000-series and Center for Internet Security (CIS) controls, in their framework. Through synthesis and analysis of ICT security tools and techniques among HEIs, this critical review hopes to provide research directions on IT governance that academic and technical administrators can further explore to secure their information resources.

KEYWORDS

information security, cybersecurity, higher education institutions, IT governance

1 INTRODUCTION

The use and reliance on information technology has increased in the 21st century. In such an era, protecting the technology infrastructure of individuals and organizations is important. In this regard, information security and cybersecurity technologies are employed. Information security protects organizations' information from unauthorized modification, disruption, inspection, and disclosure [1]–[7]. This information can be in whatever form cyber or otherwise. Information and Communication technology (ICT) Security technologies and practices specifically deal with securing organizations' digital infrastructure to help mitigate threats [8]–[11]. Such practices include employing anti-malware software,

Nuñez, M., Palmer, X.-L., Potter, L., Aliac, C.J., Velasco, L.C. (2023). ICT Security Tools and Techniques among Higher Education Institutions: A Critical Review. *International Journal of Emerging Technologies in Learning (iJET)*, 18(15), pp. 4–22. https://doi.org/10.3991/ijet.v18i15.40673

Article submitted 2023-04-18. Resubmitted 2023-05-20. Final acceptance 2023-05-21. Final version published as submitted by the authors.

firewalls, user-access controls, and network segmentation, among others [3], [12], [13]. ICT security is a unique field of research; at the same time, general laws and guidelines exist in it [11], [13]–[17], the specific requirements differ from organization to organization, and there are many potential factors that can change its implementation and adoption. Despite this, its adoption in business and organizations is crucial. ICT security tools and techniques are put in place to protect digital assets and infrastructures [3], [7], [17]–[24]. The research on this and its adoption in organizations tends to be organization-specific case studies. Implementing ICT security controls in higher-risk industries will favor more stringent security protocols over the convenience of the users and employees, whereas the ICT security policies of an educational institution will favor accessibility of information and convenience over the former.

Higher-education institutions (HEIs) provide post-secondary education to the community, and they are now greatly digitized in the 21st century leaning on technology to manage their vast amounts of information [5], [6], [17], [22], [25], [26]. Computer infrastructure and networks are put in place to assist students, faculty, and staff in the operation of the institutions. Due to the COVID-19 pandemic, HEIs have increased their adoption of technology [9], [19], [27]. Document-tracking systems (DTSs), e-libraries, and the management of classes and enrollment and learning management Systems (LMSs) are popular among HEIs to continue their education offerings despite the pandemic [19], [27]. All these technologies provide significant benefits and convenience to their constituents. However, as HEIs increase their usage of digital resources, it also puts them at higher risk of threats. HEIs that provide digital hosting of research papers face threats of intellectual property damage if an attacker decides to steal the papers [10], [15]. Sensitive documents that are tracked in DTSs can be intercepted if the DTS is compromised and leaked. Auditing systems and other digital management systems are similarly at risk. Digital methods of grading and assessing student performance are also at risk of unauthorized modification, among other threats. Any organization with a significant digital infrastructure will have to face and manage the risks from common security threats. HEIs will face both common and unique threats. In this regard, HEIs need to have a good adoption of ICT security practices to protect the institutions from said threats.

ICT security, a general term both for information security and cybersecurity, is an evolving area with unique challenges across various industries. The literature on this topic mostly comprises case studies [1], [16], [17], [20], [28]–[34]. This review aims to synthesize and evaluate existing literature on ICT security and HEIs to identify the tools, techniques, and technologies employed by HEIs and assess their adoption of ICT security measures. The study will analyze journal articles and profile cybersecurity tools and techniques used by HEIs. The focus will be on technologies used to safeguard digital assets and infrastructure, such as management tools, endpoint protection services, and networking infrastructure [6], [13], [35]–[41]. The study is targeted at HEI information and cybersecurity professionals, stakeholders, and information systems researchers. It will provide a holistic view of the state of ICT security in HEIs and allow for the development of hypotheses based on the reviewed literature. The study will evaluate key themes and issues in ICT security to gain a comprehensive understanding of the field. As this study is a critical review, it allows us to extrapolate our own hypotheses based on the literature reviewed [42]. This allows us to evaluate and critique the information gathered from the literature, making way for the understanding

of the key themes and issues of the ICT security field in a holistic manner [43]. By conducting literature profiling, synthesis of ICT security tools and techniques along with research gap analysis, this study hopes to provide inputs to HEI decision makers on prospective research work that needs to be undertaken in this body of knowledge.

2 METHODOLOGY

2.1 Literature profiling

Profiling the literature provides insight into which fields of research the topic belongs to; whether or not it falls under computer science, management, information systems, or other fields of research. The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) statement was designed to help reviewers transparently report why a review was done, what the authors of a study did, and what they found [44]. As such, the PRISMA checklist was adopted in this study, where applicable. In gathering literature, we largely used Google Scholar's search engine to look for journals. The search string used to search for literature was a combination of the terms, *cybersecurity*, *cyber security*, *information security*, *universities*, *schools*, *higher education*, and *security*. As shown in Figure 1, the search string was developed via the researcher's own knowledge and validated by comparing it to similar reviews. A study conducted a systematic review of information security management in HEIs and used similar search strings to obtain publications [45]. This yielded around 30,600 results. Selecting an appropriate sample for this study required screening the entries against eligibility criteria, ensuring that the final sample of articles to synthesize was relevant to the study. The article had to be inherently about or related to information security or cybersecurity to be eligible. Other factors involved in the eligibility criteria included the publication date, publication language, and the study's participants or sample. The publication had to be a journal article published within the decade 2012–2022 and be targeted to HEIs or have HEIs as participants or samples. This resulted in a list of 150 publications. Additionally, the article had to be published in a journal indexed in the Scimago journal rank, which references Elsevier's Scopus database of journal articles, and the article had to have content on cybersecurity tools and technologies employed in HEIs. One journal article was exempted from the publication date criteria because while it was started in 2005, its research is ongoing [36]. We deemed this a valid reason to include the journal article in the sample. These criteria reduced the final sample size of journal articles to 11, as shown in the Appendix.

To gain a better understanding of the literature, we then proceeded to profile the journal articles according to their authors' background, publication year, and the SciMago categories and subject areas of the journal that the article belonged to. We also performed our own thematic analysis of the journal articles. Open-source intelligence is used to gather information about the authors of the articles. Information sought included their country of residence, highest education level and other credentials, research disciplines, and affiliations to universities and institutions. The Scimago Journal Rank provided information about the journals' category and subject areas while our own thematic analysis was performed through qualitative coding.

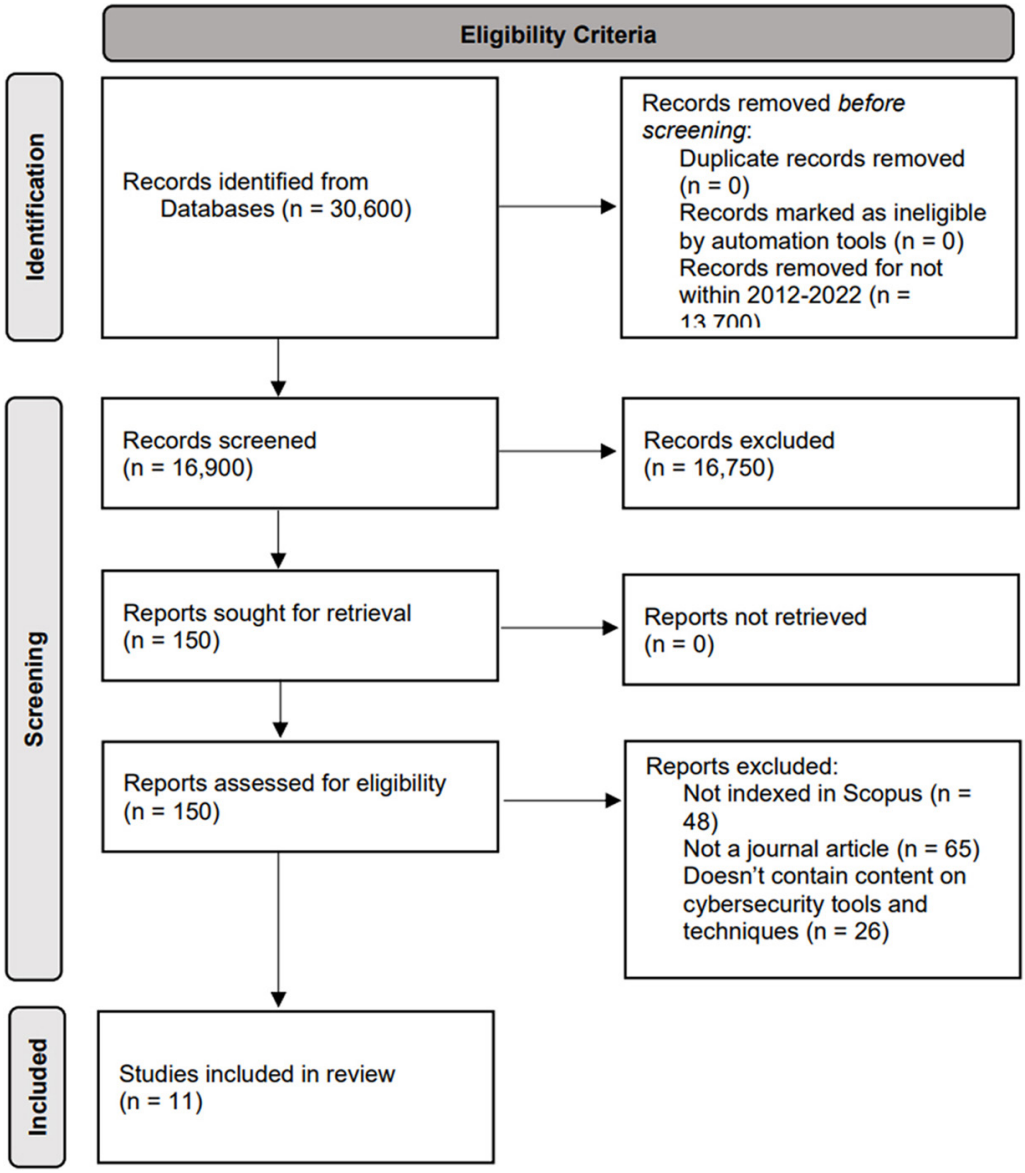

Fig. 1. Flowchart of the article of the selection process according to PRISMA 2020 statement [44, 46]

2.2 Synthesis of ICT security tools and techniques

After the articles were screened and profiled, we proceeded to synthesize information regarding the ICT security tools and techniques that HEIs use according to information found in the sample size of journal articles. The 11 journal articles were analyzed through inductive coding, keeping in mind the objective of this study: to find out what tools and techniques HEIs employ for ICT security. Specifically, we aimed to synthesize the types of ICT security threats that are identified in HEIs, control methodologies to secure their infrastructure against those threats and draw recommendations from the literature. As shown in Figure 2, we categorized the control methodologies that HEIs employ into four categories. Three of these - organizational, technological, and physical security - were adopted from Singh and Margam's 2018 paper on Information Security Measures of Libraries

of Central Universities of Delhi, in which they categorized quantitatively the threats into the categories [13]. This method of categorization separates the threats according to the vulnerable entity of organizations. Additionally, we hypothesized that HEIs approach to ICT security is like that of most organizations, as they use well-known and recognized organizational standards and frameworks. We added a fourth category: Standards and Frameworks. This category encompasses the well-known and recognized organizational standards and frameworks that an organization can use to protect its cyberinfrastructures, such as those from the International Organization for Standardization (ISO) and the Center for Internet Security (CIS).

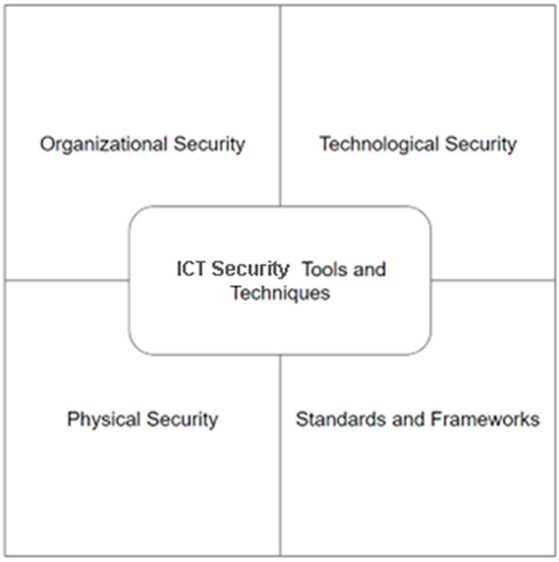

Fig. 2. Categorization of ICT security tools and techniques

Organizational security deals with threats that result from vulnerabilities in the HEI's management of human and digital assets. Human risks are also a major contributing factor to an organization's security. This is especially true in HEIs, which are in many countries chronically underfunded, especially in auxiliary/support positions like IT. Additionally, an HEIs faculty tends to have older employees, for whom IT knowledge is not easily grasped. Improper access management of personnel can put the organization at risk for insider threats. Personnel with little training and awareness of security practices are also considered a risk to an organization's ICT security infrastructure. Among the risk factors, human factors are considered the weakest link [47], [48]. Technological security deals with threats that stem from vulnerabilities in the application, software, and networking systems that the organization uses. These vulnerabilities can result in Structured Query Language (SQL) injection attacks, Cross-Site Request Forgery (CSRF attacks, and sniffing attacks, to name a few [38]. Threats in the network arise from vulnerabilities rooted in interconnected devices, especially those connected to the internet. Improperly configured networking and servers can give an attacker unauthorized access to the institution's computers and databases [48]. Meanwhile, physical security deals with securing the data communication infrastructure with physical means. Data centers, servers, networking equipment, computers, and the like need to be protected against physical threats. These threats can come in the form of flooding, fire, earthquakes, theft, robbery, and physical damage [13], [35], [39]. Due to this, we believe that physically

securing an organization's data communication infrastructure is equally as important as securing it in the digital space.

2.3 Research gap analysis

This section discusses the gaps in the literature of HEI ICT security. The gaps are identified after thoroughly evaluating and critiquing the Conclusions and Recommendations sections of the 11 eligible articles through open coding. Common limitations of the literature were also included in the evaluation. Understanding these research gaps is important as it provides insight into unexplored or underexplored areas within the field. Additionally, research gaps provide information on where the current research and literature fall short. Hence, the research gaps identified in this critical review may be pursued in future research. Some gaps will likely be unfilled for very good reasons since it is expected that there is probably a lot of information that would never be published about cyberthreats in HEIs. There is considerable vested interest in not going public with a threat, and many HEIs have no legal compulsion to disclose hacks unless privileged information is accessed. Many unexplored areas of interest could also be the motive for a cyberattack. Student records could contain potential blackmail material, but hackers wouldn't be able to use it very quickly-they would have to wait until the student had enough money to be worth blackmailing. Additionally, most universities outsource their class materials (Moodle, Canva, Blackboard) so they likely have less control on their protection methods against ransomware.

3 METHODOLOGY

3.1 Literature-profiling results

There was a total of 29 authors involved in the sample of journal articles used in this study (Figure 3). Most of the authors had PhD degrees. Notably, 1 of these authors also had a reputable certification in IT practices, Cisco Certified Network Associate (CCNA), certifying that the holder had. a working foundational expertise in the field of IT. The drastic contrast between the number of authors with PhDs and authors with IT certifications indicates that there are a minute number of IT professionals writing research papers about Information security and cybersecurity; instead, these papers are written and published predominantly by academicians. This can further indicate a gap between industry and the academe.

The literature was also profiled according to the geographic location of the authors. Most of these authors resided in Asia and Europe. The location was based on larger regions to increase the differentiation between geographic characterization of the literature, as a more specific categorization would not be helpful for this sample size of eligible literature. As shown in Figure 4, profiling of the geographic differences between the authors shows that Asia had the highest number of publications, closely followed by Europe, Africa, and the United States. Based on this, it could be hypothesized that among the five, Asia has the highest interest in the cybersecurity of its HEIs, with the United States having the least. However, we believe that this data is not representative of the research and that other factors such as sample size must have affected the data. This could also be ascribed to the relatively lower level of national funding that the US supplies to universities whose cost is mostly supported by student tuition.

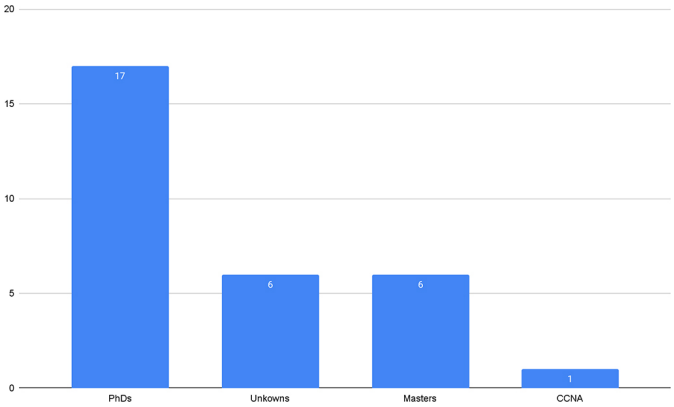

Fig. 3. Authors' credentials

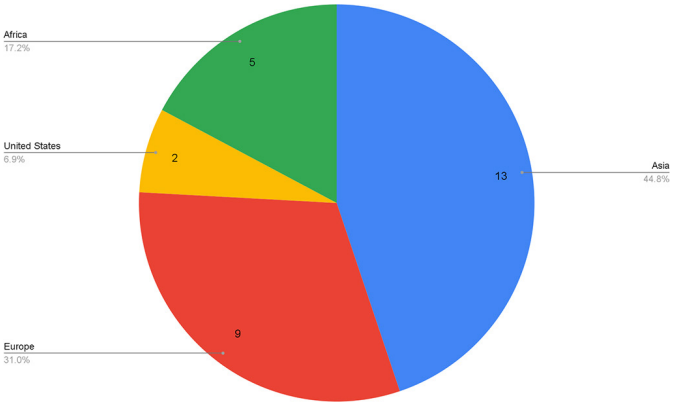

Fig. 4. Authors' locations

Further, the literature was profiled according to the year of publication. The years 2014 and 2019 saw the greatest number of publications; 2012 and 2022 saw the least. Figure 5 graphically shows that the increased number of publications in 2019 can be attributed to growing concerns over HEI's ICT security with the onset of the COVID-19 pandemic [47]. Additionally, the linear regression of the data, as shown in Figure 6 shows that the frequency of publications has a slight positive association between the number of publications and the later, the year of publication. This indicates an increasing interest in the field of HEI cybersecurity, likely stemming from HEIs' increasing reliance on digital infrastructure.

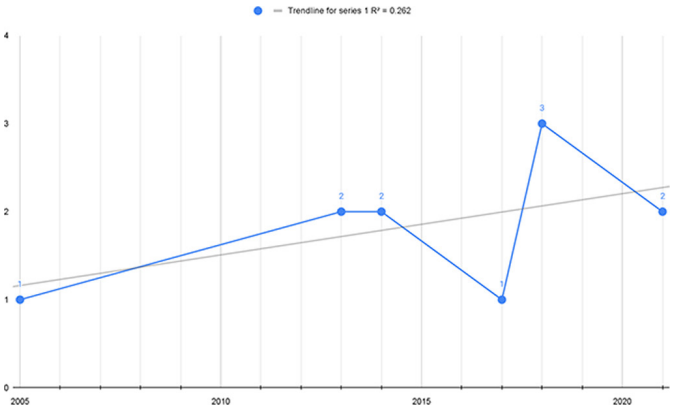

Fig. 5. Number of publications by year

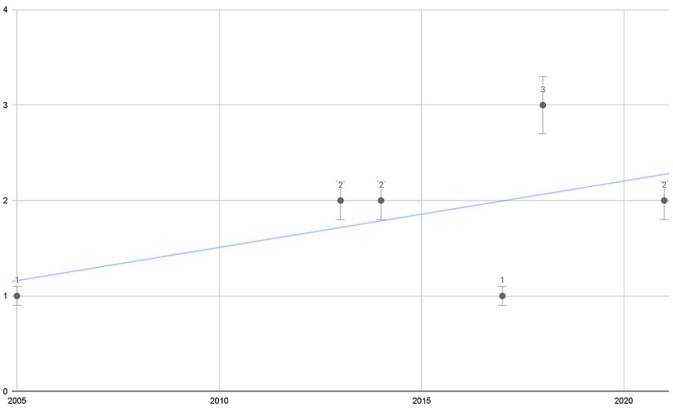

Fig. 6. Linear regression of publications by year

The articles were also profiled according to the journals in which they were published. The Scimago journal rank provides information on the journal's category and subject areas and was consequently used to profile the articles. The journals' categories provide insight into which field of research HEI ICT security generally falls under, while the subject areas provide insight into what specific topics are usually covered by the journal articles. The sample of eligible journal articles was spread across 9 different Scopus-indexed journals. The Appendix is a list of eligible journal articles. These journals were also published in 5 different categories and 12 different subject areas. Among the 5 categories, it was found that the journals mainly fell under computer science, engineering, and social science, as illustrated in Figure 7. The 3 leading subject areas were computer science (miscellaneous), engineering, and library and information sciences, as shown in Figure 8.

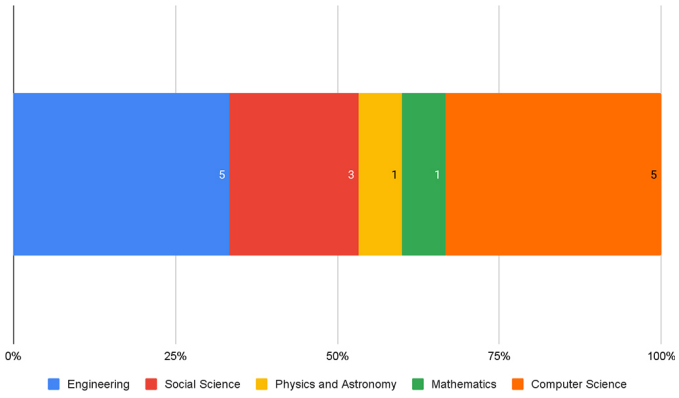

Fig. 7. Journal categories

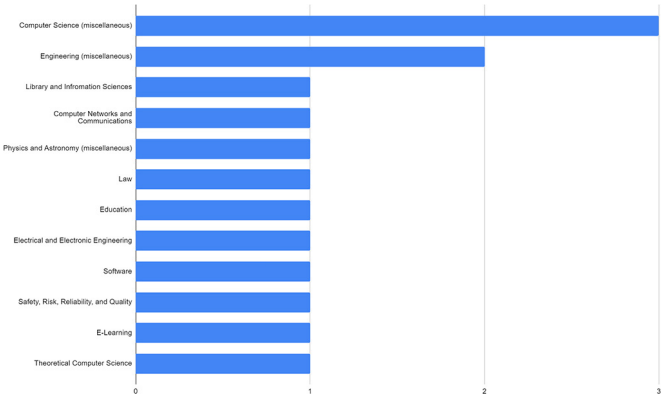

Fig. 8. Journal subject areas

3.2 Synthesis results of ICT security tools and techniques

Through open coding, we tallied the number of times an article states what information security and cybersecurity tools and techniques HEIs employ. As Figure 9 depicts, the literature shows that HEIs employ technological security measures the most, followed by observation of standards and frameworks, organizational security measures, and lastly physical security measures. Technological security appeared (43) times in (6) journals, with emphasis on endpoint security and network security [13], [35]–[39]. Organizational security appeared (27) times in (6) journals that emphasized policymaking [6], [13], [35], [38], [48], [49]. Standards and frameworks came next, (16) times in (4) journals [6], [36], [40], [41], and physical security came last, 8 times in (3) journals. The high number of technological security measures could be due to its technological nature. The trend of observing ICT security standards and frameworks among HEIs further supports our hypothesis that HEIs approach to ICT security is like that of organizations outside academia. The focus on technological areas could also explain the low observance of physical security measures.

The results of the open-coding analysis show that HEIs employ technological security measures the most, followed by observation of standards and frameworks, organizational security measures, and physical security measures. This finding suggests that HEIs prioritize protecting their infrastructure through technological means, such as endpoint security and network security. This is likely due to the technological nature of the security threats and the fact that HEIs are heavily reliant on technology to operate. Additionally, the high usage of ICT security standards and frameworks among HEIs suggests that they approach ICT security in a similar manner to other organizations outside of academia. This is an important finding because it suggests that HEIs can benefit by adopting best practices and standards from other industries. The inadequate implementation of physical security measures may raise concerns. While technological security measures are crucial to safeguarding against cyber threats and data breaches, physical security measures are equally crucial in preventing unauthorized access to sensitive information and equipment. The underutilization of physical security measures could be attributed to the misconception that cybersecurity threats are solely technological in nature. HEIs should ensure that they have sufficient physical security measures in place to counter physical attacks or breaches. In conclusion, these findings can guide HEIs' ICT security strategies, aiding them in prioritizing their resources and efforts towards protecting against cyber threats.

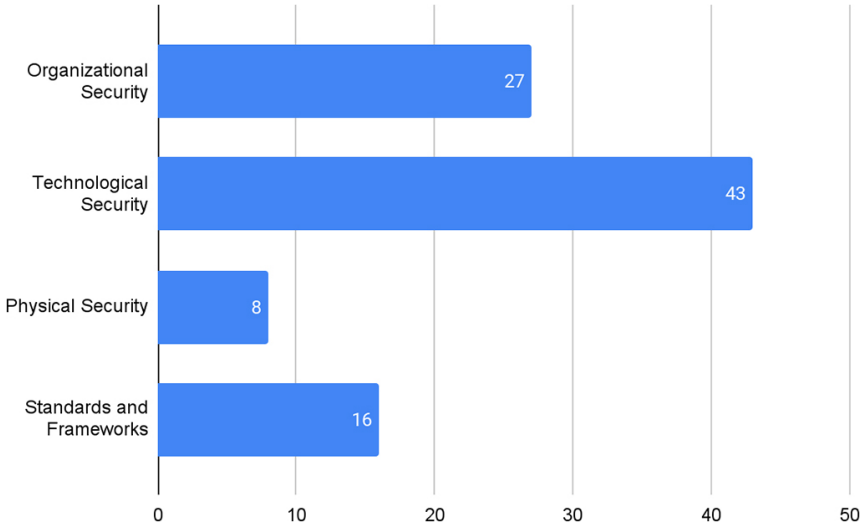

Fig. 9. ICT security methodologies by category

Organizational security. With the threats and risk factors identified in Section 2.2, the tools and techniques employed to protect against them are synthesized from the literature through open coding. Table 1 shows that the methods employed for organizational security commonly involve implementing policies that the organization's employees must abide by. Three articles state the use of policies that include security policies; password policies; hardware policies; and policies on storing, sharing, and transmission of data [13], [35], [49]; 1 article states the use of policies on the classification of data and sensitive information [48]. In addition, 4 articles state the use of staff training, raising ICT security awareness, and risk-management plans as part of their organizational security [6], [35], [38], [49]. Policies that deal with the security of an organization have become significant corporate documents that aid in the protection of an organization's ICT security infrastructure [40]. Such policies guide an organization's personnel in the dos and don'ts when interacting with digital assets and infrastructure. However, we believe that the existence of policies is merely half of the equation. Management must also track and enforce the compliance of these policies for them to be effective. This is notoriously difficult, as in some HEIs, the institution of tenure makes it exceptionally difficult to coerce a staff member into doing something that they do not see as necessary. This implies that personnel who are non-compliant with what ought to be very basic IT rules and regulations cannot be easily or quickly removed. In turn, gaps in cybersecurity procedures may persist in HEIs, without easy rectification. Additionally, while it takes time to learn proper IT procedures such as proper data management, the mass of workers at an HEI are not long-term employees, but students. As their main goal is to leave the institution, which usually pays little above poverty wages, they are not motivated to follow IT rules. Contrast this with a government-sponsored lab, where workers are paid more equitably, have longer employment stays, and therefore have far fewer incidents of data breaches, despite having far more valuable information from a data-gathering perspective. Organizations need to apply broad directives pertaining to their IT strategy and offer guidelines for making decisions. However, organizations are not required to concentrate on the specifics of implementation. The primary goal of policies is to convey an organization's values, culture, and IT philosophy. A good policy clarifies the guidelines and arranges them logically.

Table 1. Summary of HEI organizational security methods

Organizational Security	Journal Articles	Count
Security policies	[13], [35], [49]	3
Password policies	[13], [35], [49]	3
Hardware policies	[13], [35], [49]	3
Policies on storing, sharing, and transmission of data	[13], [35], [49]	3
Policies on the classification of data and sensitive information	[48]	1
Staff training	[6], [35], [38], [49]	4
Raising cybersecurity awareness	[6], [35], [38], [49]	4
Risk-management plans	[6], [35], [38], [49]	4

Technological security. Regarding the aspect of technological security, endpoint protection services are commonly employed [13], [35]–[37]. Kaspersky defines endpoint security as systems that protect system endpoints desktops, laptops, mobile devices, and other terminals. This is done to prevent cybercriminals from using them as points of entry into the system or network. Endpoint security, is composed of different technologies that work together. Table 2 shows that 5) articles mention the use of firewalls, antimalware, data encryption, insider threat protection, and web-browsing protection [13], [35]–[38]. Since very few universities can afford to subscribe to all extant scientific journals, it is possible that researchers at an HEI would be forced to use unsafe web-browsing practices. The implication is that this opens another window for a data breach. Technological security also includes the networking infrastructure of the institutions [35], [37]–[39]. Securing the network is of vital importance to any organization's cybersecurity strategy. Multiple reports mention how a network can easily infect computers and spread viruses to them when improperly configured. Infowatch's 2014 report states that 38% of data leaks are done through network vulnerabilities [50]. Kaspersky states that 61% of attacks on home users came from attacks that exploit internet browsers [50]. In this regard, the same 5 articles state that HEIs employ network intrusion detection, server protection, firewalls, VLANs, and network isolation to protect their networking infrastructure [35], [37]–[39]. Network security is, without a doubt, crucial for the technological security of an organization. While endpoint protection services and network security largely make up the technological security of HEIs, it is noteworthy that services such as antimalware and web-browsing protection are at peak efficiency only if their recognition databases are kept up to date. Otherwise, such services fall behind when new types of malware find their way into the infrastructure. There are, however, antimalware services that employ artificial intelligence (AI) technology to protect against previously unknown types of attacks, also known as zero-day attacks [50]. In other words, we hypothesize that the efficiency of technological security tools can vary greatly, depending on the software's vendor and how the software is implemented.

Table 2. Summary of HEI technological security methods

Technological Security	Journal Articles	Count
Firewalls	[13], [35]–[38]	5
Antimalware software	[13], [35]–[38]	5
Data encryption	[13], [35]–[38]	5
Insider threat protection	[13], [35]–[38]	5
Web-browsing protection	[13], [35]–[38]	5
Network-intrusion detection	[35], [37]–[39]	4
Server protection	[35], [37]–[39]	4
VLANs	[35], [37]–[39]	4
Network isolation	[35], [37]–[39]	4

Physical security. When it comes to the management of a cyber infrastructure's physical security, the protection of the organization's networking devices and equipment is commonly prioritized [13]. Table 3 shows that 1 article states the employment of the following measures to prevent physical damage to an HEI's cyberinfrastructure: temperature control, disaster early warning systems, sprinklers, smoke detectors, fireproofing, and the protection of entrances and exits. [13]. Two articles also state that physical isolation of public-facing and sensitive networks is an option for institutions handling higher-risk information [35], [39]. In the case of HEIs, this can be applied to databases that deal with personally identifiable information (PII). Seeing how the number of tools regarding physical security is low, we believe that the importance of physical security of HEIs' cyberinfrastructure is largely underestimated. This is especially true as most university labs are reliant on low- or non-paid staff members, some of whom lack full documentation for their position. Whether this situation should be considered acceptable for cost-cutting or as standard practice in HEIs is debatable but not the subject of this paper. It is, however, a means by which a hack can be instigated very effectively. This can prove to be fatal, as no amount of digital protection mechanisms can prevent a dedicated intruder from potentially breaking into the institution's server room and stealing sensitive information or from doing other damage to the cyber infrastructure.

Table 3. Summary of HEI physical security methods

Physical Security	Journal Articles	Count
Temperature control	[13]	1
Disaster early warning system	[13]	1
Sprinklers	[13]	1
Smoke detectors	[13]	1
Fireproofing	[13]	1
Protection of entrances and exits	[13]	1
Physical isolation of networks	[35], [39]	2

Standards and frameworks. As hypothesized by us, HEIs also make use of standardized cybersecurity frameworks and standards to protect their cyberinfrastructure. Table 4 shows that common frameworks are the ISO 27000-series, Control Objectives for Information and Related Technologies (COBIT), Center of Internet Security (CIS) Controls, and National Institute of Standards and Technology's (NIST)

Cybersecurity Framework [6], [36], [40], [41]. Often, these standards and frameworks consider all the categories of cybersecurity that are defined in this article. However, these standards still require interpretation, and since some HEIs have underfunded support staff, they may not be up to that task. Non-IT staff still require implementation and training. This means that while these standards are well established and well conceived, they still require personnel to interpret them and adhere to them.

Table 4. Summary of HEI standards and frameworks

Standards and Frameworks	Journal Articles	Count
ISO 27000-series	[6], [36], [40], [41]	4
COBIT	[6], [36], [40], [41]	4
CIS Controls	[6], [36], [40], [41]	4
NIST	[6], [36], [40], [41]	4

Table 5 shows that 1 paper states that there are tools and techniques that span both organizational and technological security that are also employed: identity assurance and authorship assurance [48]. Identity assurance consists of identity document verification, password-based authentication, question-based identity verification, physical biometrics, and behavioral biometrics. Authorship assurance comprises plagiarism detection, traditional proctoring, remote proctoring, behavioral biometrics, instructor validation, computer lockdowns, instructional design, and the employment of organizational policies [48].

Table 5. Additional HEI organizational and technological security methods

Identity Assurance	Authorship Assurance
Identity document verification	Plagiarism detection
Password-based authentication	Traditional proctoring
Question-based identity verification	Remote proctoring
Physical biometrics	Behavioral biometrics
Behavioral biometrics	Instructor validation

3.3 Research gap analysis results

Figure 10 summarizes the cybersecurity tools and techniques, showing the areas of concerns that HEIs are currently addressing. Most of the articles in the literature conclude that the use of various organizational, technological, and physical security strategies can significantly improve the cybersecurity of HEIs [6], [13], [35], [36], [38], [40], [41], [48], [49]. It is clear that the categories of ICT security tools and techniques defined in this critical review are crucial in the protection of HEI's cyberinfrastructure. Additionally, the use of standards and frameworks such as the ISO27001:2013 [36], [40] and COBIT5 [36] standards can greatly improve HEIs cybersecurity [36], [40], [41], supporting our inclusion of the Standards and Frameworks category in identifying ICT security tools and techniques employed in HEIs. However, this type of security is not without its flaws. Singh and Margam's 2018 journal article states that the physical security aspect is lagging among HEIs, supporting the hypothesis and data synthesized in our review [13]. Weaknesses in HEIs' policymaking were identified [36], [38],

[38], [40], as well as other organizational security flaws such as poor cybersecurity awareness among the HEIs' constituents [35], [49]. Notably, gaps in HEIs' implementation of ISO27001:2013 and COBIT5 were identified as increasing the security risks at HEIs [36]. Further, in line with our objectives of performing this critical review, there's no clear globally accepted process for implementing cybersecurity measures among HEIs, as supported by Ghazvini et al. [40]. To mitigate risk, it is recommended that HEIs put more effort into the policy-making process [36], [38], [38], [40], alongside other organizational security measures [35], [49]. HEIs should also improve staff training and organize cybersecurity awareness campaigns for their constituents [36]. The IT and security teams of HEIs should also be implementing modern technical measures to protect the cyberinfrastructure of HEIs [13], [35], [39].

After performing the gap analysis, we believe that the research gaps identified in the literature coincide with the hypotheses and inferences drawn in this critical review. However, our review only scratches the surface of the transformational changes that need to occur to secure the future of IT in HEIs. One needed reform is that the fundamental mindset of a university insofar as information security ought to change. Manuscripts can still be published, classes still distributed, and knowledge still disseminated, but PII and other privileged information needs to be protected, and the importance of protecting this information ought to be instilled in every staff member. To do this, many institutions need to change. For instance, violations of IT policy ought to be violations that are fineable—even with tenure—workers ought to receive compensation that makes them care about the long-term success of the HEI, and support staff ought to be seen as integral personnel. This last point may change IT requirements from being presented as a pre-recorded class that is viewed once a year to having ongoing updates from IT staff to the greater university community.

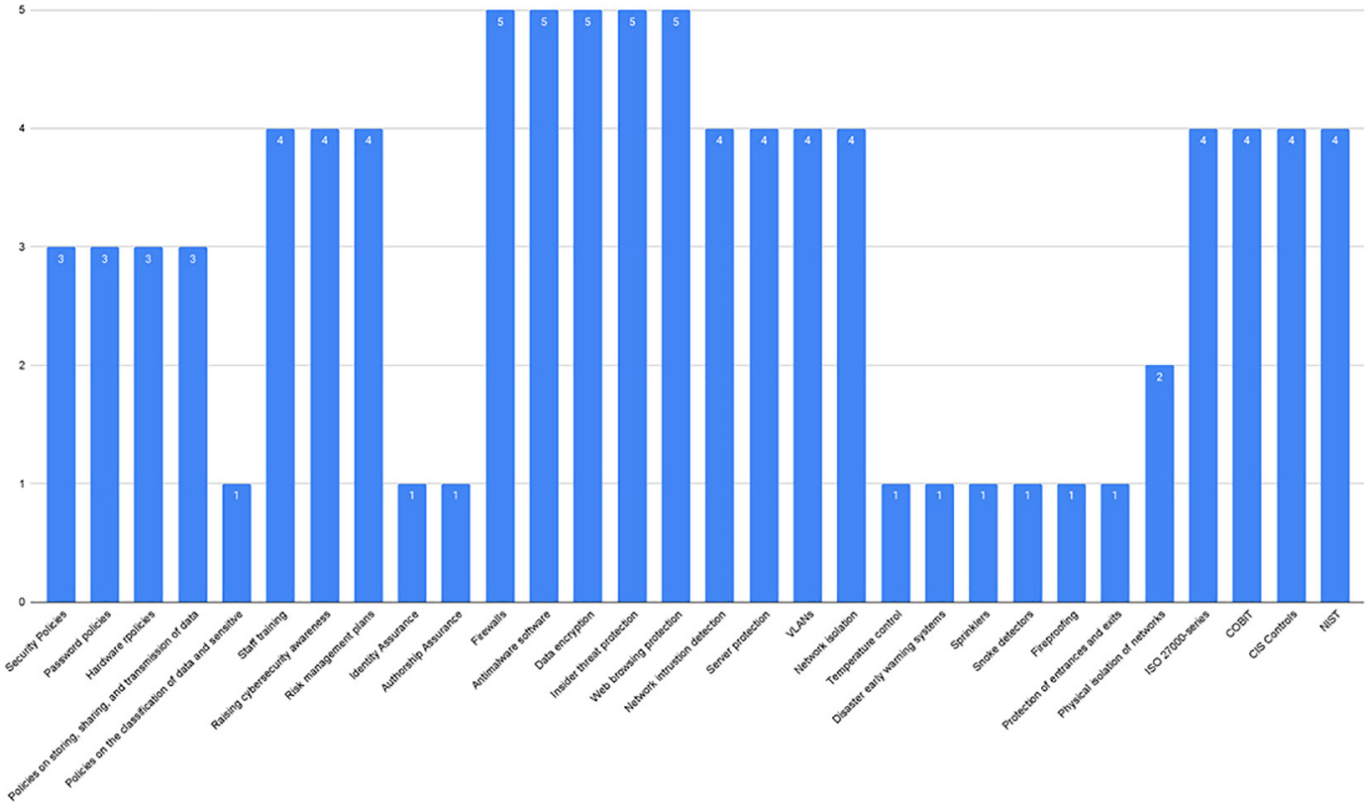

Fig. 10. ICT security tools and techniques employed in HEIs

4 CONCLUSION AND RECOMMENDATIONS

This study took on the research questions that ask about the ICT security threats that exist in HEIs and the tools and techniques that institutions put in place to counter these threats. Literature was gathered and screened, resulting in a sample of 11 eligible journal articles. These articles were then profiled according to information about their authors and the articles' content. Open coding was then performed on the eligible articles to come up with a list of the cyber threats of HEIs as well as the tools and techniques that HEIs employ against these threats. During the profiling, it was found that most of the authors had obtained a PhD but that few of them have cybersecurity certifications from reputable issuers. From this, it can be drawn that the expertise of the authors of the eligible journal articles is primarily of academic quality. Furthermore, most of the authors were from Asia, followed by Europe. The skew of representation leaves out perspectives outside of Americas and Africa, which may have different systems in place. As a result, the information raised is of more limited relevance to users outside of those regions that have systemic incompatibilities. This potentially leaves out DIY/in-house organizational perspectives. A regression analysis on the publication years of the eligible papers showed a positive correlation between the number of publications and the publication year, implying that research interest in the field of information security and cybersecurity of HEIs is increasing.

Open coding of the sample literature found that cybersecurity threats to HEIs' security infrastructure target organizational, technological, and physical vulnerabilities. Hence, various organizational, technological, and physical security measures are commonly employed to counter these threats. There is a long list of security measures that deal with the human factor of IT risk, implying that the human factor is a high risk to an institution's ICT security—in line with the current literature. A number of organizational and technological security methods were also found to work together in managing the identity and authorship assurance of the organization. Further, it was found that HEIs employ the use of well-established standards and guidelines despite them not being specifically designed and used by HEIs. The common use of such standards can imply that HEIs treat themselves similarly to a typical organization when managing their technological security.

The importance of this study lies in its ability to identify the ICT threats present in HEIs as well as the tools and techniques utilized to combat these threats. Through the analysis of 11 relevant journal articles and the process of open coding, this study successfully determined the common vulnerabilities in HEIs' ICT security infrastructure and the security measures employed to address them. The study's results offer useful guidance to HEIs for the development of more effective strategies to ensure the safety of their data and systems. One significant finding of this study is the role of the human factor in an institution's ICT security, which highlights the importance of educating and training staff and students on the institution's best practices. Additionally, the study reveals that HEIs typically implement well-established ICT security standards and guidelines, indicating the potential benefits of adopting existing practices and standards from other industries. Nevertheless, the study acknowledges a limitation in its focus on Asia and Europe, which excludes HEIs from other regions. Thus, future research should consider a broader perspective to provide a more comprehensive understanding of information security and cybersecurity threats and solutions in HEIs worldwide. In summary, this study provides valuable insights into the current state of ICT security in HEIs, which can inform future research and practices in this critical field.

5 REFERENCES

[1] M. Magomelo, P. Mamboko, and T. Tsokota, "The Status of Information Security Governance within State Universities in Zimbabwe," vol. 5, no. 8, 2014.

[2] D. E. Marcial, "IT Security In The Higher Education Institutions," J. Inform., vol. 8, no. 1, 2012, https://doi.org/10.21460/inf.2012.81.110

[3] X. Liu, "Design and Development of a Web-based Platform to Manage Information Resources security in Higher Education", University of North Carolina, Carolina Digital Repository, 2018, https://doi.org/10.17615/ctj1-6v49

[4] A. Abdelwahed, A. Mahmoud, and R. Bdair, "Information Security Policies and their Relationship with the Effectiveness of the Management Information Systems of Major Palestinian Universities in the Gaza Strip," Int. J. Inf. Sci. Manag., vol. 15, no. 1, 2017.

[5] S. Hina and P. D. D. Dominic, "Information Security Policies: Investigation of Compliance in Universities," in 2016 3rd International Conference on Computer and Information Sciences (ICCOINS), Kuala Lumpur, Malaysia, 2016. https://doi.org/10.1109/ICCOINS.2016.7783277

[6] S. Faris, S. E. Hasnaoui, H. Medromi, H. Iguer, and A. Sayouti, "Toward an Effective Information Security Risk Management of Universities' Information Systems Using Multi Agent Systems, Itil, Iso 27002, Iso 27005," Int. J. Adv. Comput. Sci. Appl., vol. 5, no. 6, 2014, https://doi.org/10.14569/IJACSA.2014.050617

[7] T. A. Eze and C. C.-E. Aroh, "Management of Information Security in Public Universities in Nigeria," Int. J. Digit. Soc., vol. 11, no. 1, pp. 1575–1578, 2020, https://doi.org/10.20533/ijds.2040.2570.2020.0196

[8] I. Piscikiene, J. Romeikiene, and B. Šustickienė, "Cyber Vulnerability in Light of Online Learning Reality," Soc. Integr. Educ. Proc. Int. Sci. Conf., vol. 5, pp. 426–435, 2021, https://doi.org/10.17770/sie2021vol5.6367

[9] Rajesh Chandarman and Brett Van Niekerk, "Students' Cybersecurity Awareness at a Private Tertiary Educational Institution," Afr. J. Inf. Commun. AJIC, no. 20, 2017, https://doi.org/10.23962/10539/23572

[10] B. Badamasi and S. C. A. Utulu, "Framework for Managing Cybercrime Risks in Nigerian Universities," In Proceedings of the 1st Virtual Conference on Implications of Information and Digital Technologies for Development, 2021.

[11] D. Anderson, O. P. Abiodun, and A. Christoffels, "Information security at South African universities—implications for biomedical research," Int. Data Priv. Law, vol. 10, no. 2, pp. 180–186, 2020, https://doi.org/10.1093/idpl/ipaa007

[12] M. Schuett and S. S. M. Rahman, "Information Security Synthesis in Online Universities," Int. J. Netw. Secur. Its Appl., vol. 3, no. 5, pp. 1–20, 2011, https://doi.org/10.5121/ijnsa.2011.3501

[13] V. Singh and M. Margam, "Information Security Measures of Libraries of Central Universities of Delhi : A Study," DESIDOC J. Libr. Inf. Technol., vol. 38, no. 2, p. 102, 2018, https://doi.org/10.14429/djlit.38.2.11879

[14] A. Aliyu et al., "A Holistic Cybersecurity Maturity Assessment Framework for Higher Education Institutions in the United Kingdom," Appl. Sci., vol. 10, no. 10, p. 3660, 2020, https://doi.org/10.3390/app10103660

[15] I. Bandara, C. Balakrishna, and F. Ioras, "The Need for Cyber Threat Intelligence for Distance Learning Prividers and Online Learning Systems," presented at the 15th International Technology, Education and Development Conference, Online Conference, Mar. 2021, pp. 9312–9321. https://doi.org/10.21125/inted.2021.1947

[16] K. Bálint, "Possibilities for the Utilization of an Automatized, Electronic Blockchain-based, Students' Attendance Register, using a Universities' Modern Security Cameras," Acta Polytech. Hung., vol. 18, no. 2, pp. 127–142, 2021, https://doi.org/10.12700/APH.18.2.2021.2.7

[17] L. May and T. Lane, "A Model for Improving e-Security in Australian Universities," J. Theor. Appl. Electron. Commer. Res., vol. 1, no. 2, pp. 90–96, 2006, https://doi.org/10.3390/jtaer1020016

[18] Y. M. Iriqat, A. R. Ahlan, and N. N. A. Molok, "Information Security Policy Perceived Compliance Among Staff in Palestine universities: An Empirical Pilot study," in 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), Amman, Jordan, Apr. 2019, pp. 580–585. https://doi.org/10.1109/JEEIT.2019.8717438

[19] S. Cohney, R. Teixeira, A. Kohlbrenner, A. Narayanan, M. Kshirsagar, Y. Shvartzshnaider, M. Sanfilippo, "Virtual Classrooms and Real Harms: Remote Learning at U.S. Universities," Cornel University, 2020.

[20] B. Mutunhu, D. S. Dube, N. Ncube, and S. Sibanda, "Cyber Security Awareness and Education Framework for Zimbabwe Universities: A Case of National University of Science and Technology," 2022.

[21] J. Wang, "Information Security Governance in Colleges and Universities," DEStech Trans. Econ. Bus. Manag., no. icem, Sep. 2017, https://doi.org/10.12783/dtem/icem2017/13206

[22] D. Makupi, "A Design of Information Security Maturity Model for Universities Based on ISO 27001," Int. J. Bus. Manag., vol. 7, no. 6, 2019, https://doi.org/10.24940/theijbm/2019/v7/i6/BM1906-038

[23] W. Di, "Analysis and Countermeasure on Information Security in Universities," in 2020 IEEE 3rd International Conference of Safe Production and Informatization (IICSPI), Chongqing City, China, Nov. 2020, pp. 439–442. https://doi.org/10.1109/IICSPI51290.2020.9332466

[24] C. N. Hung, M. D. Hwang, and Y. C. Liu, "Building a Maturity Model of Information Security Governance for Technological Colleges and Universities in Taiwan," Appl. Mech. Mater., vol. 284–287, pp. 3657–3661, 2013, https://doi.org/10.4028/www.scientific.net/AMM.284-287.3657

[25] N. M. Almadhoun, P. D. D. Dominic, and F. W. Lai, "Investigation of Perceived Security, Privacy and Trust on Social Networking Sites for Stakeholder Relationships Development in Malaysian Universities," Int. J. Bus. Inf. Syst., vol. 15, no. 1, p. 1, 2014, https://doi.org/10.1504/IJBIS.2014.057962

[26] S. M. Lausa, "Operational Efficiency of Information Technology and Organizational Performance of State Universities and Colleges in Region VI, Philippines," vol. 4, no. 4, 2016.

[27] N. R. Mosteanu, "Digital University Campus—Change the Education System Approach to Meet the 21st Century Needs," Eur. J. Hum. Resour. Manag. Stud., vol. 4, no. 4, 2020, https://doi.org/10.46827/ejhrms.v4i4.959

[28] A. Nasir, R. Abdullah Arshah, and M. R. Ab Hamid, "A Dimension-Based Information Security Culture Model and Its Relationship With Employees' Security Behavior: A Case Study in Malaysian Higher Educational Institutions," Inf. Secur. J. Glob. Perspect., vol. 28, no. 3, pp. 55–80, 2019, https://doi.org/10.1080/19393555.2019.1643956

[29] O. S. Olorunsola, F. N. Ogwueleka, and A. E. Evwiekpaefe, "Assessment of Privacy and Security Perception of Biometric Technology Case Study of Kaduna State Tertiary Academic Institutions," Secur. Priv., vol. 3, no. 5, 2020, https://doi.org/10.1002/spy2.124

[30] E. D. Kundy, "Cyber Security Threats in Higher Learning Institutions in Tanzania, a Case of University of Arusha and Tumaini University Makumira," Olva Academy-School of Researchers, vol. 2, no. 3, 2019.

[31] S. A. Shonola, M. S. Joy, S. A. Shonola, and M. S. Joy, "Learners' Perception on Security Issues in M-learning (Nigerian Universities Case Study)," Exch. Interdiscip. Res. J., vol. 2, no. 1, pp. 102–122, 2014, https://doi.org/10.31273/eirj.v2i1.103

[32] S. A. Shonola and M. Joy, "Mobile Learning Security Issues from Lecturers' Perspectives (Nigerian Universities Case Study)," In: International Conference on Education and New Learning Technologies (EDULEARN14), Barcelona, Spain, 2014. https://doi.org/10.1109/IMCTL.2014.7011125

[33] S. S. Alotaibi and B. M. E. Elnaim, "Risks Faces the Universities of Kingdom of Saudi Arabia in Mobile Learning," Int. J. Innov., vol. 14, no. 7, 2020.

[34] C. R. Harrell, M. Patton, H. Chen, and S. Samtani, "Vulnerability Assessment, Remediation, and Automated Reporting: Case Studies of Higher Education Institutions," in 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), Miami, FL, Nov. 2018, pp. 148–153. https://doi.org/10.1109/ISI.2018.8587380

[35] Z. Huang, "An Analysis of Information Security and Protection Strategies in Colleges and Universities in the Environment of Smart Campuses," J. Phys. Conf. Ser., vol. 1852, no. 4, p. 042050, 2021, https://doi.org/10.1088/1742-6596/1852/4/042050

[36] W. Gunawan, "Measuring Information Security and Cybersecurity on Private Cloud Computing," Journal of Theoretical and Applied Information Technology, 2019, vol. 97. no 1.

[37] Y. Xu, "Research on Computer Network Security Architecture of Universities in China," Adv. Mater. Res., vol. 765–767, pp. 1486–1489, 2013, https://doi.org/10.4028/www.scientific.net/AMR.765-767.1486

[38] C. Joshi and U. K. Singh, "Information Security Risks Management Framework—A Step Towards Mitigating Security Risks in University Network," J. Inf. Secur. Appl., vol. 35, pp. 128–137, 2017, https://doi.org/10.1016/j.jisa.2017.06.006

[39] Y. Zhao, "Applied-Information Technology in the Internet of Things in the Construction of File Security System in Colleges and Universities," Adv. Mater. Res., vol. 1014, pp. 399–403, 2014, https://doi.org/10.4028/www.scientific.net/AMR.1014.399

[40] A. Ghazvini, Z. Shukur, and Z. Hood, "Review of Information Security Policy based on Content Coverage and Online Presentation in Higher Education," Int. J. Adv. Comput. Sci. Appl., vol. 9, no. 8, 2018, https://doi.org/10.14569/IJACSA.2018.090853

[41] J. Merchan-Lima, F. Astudillo-Salinas, L. Tello-Oquendo, F. Sanchez, G. Lopez-Fonseca, and D. Quiroz, "Information security management frameworks and strategies in higher education institutions: a systematic review," Ann. Telecommun., vol. 76, no. 3–4, pp. 255–270, 2021, https://doi.org/10.1007/s12243-020-00783-2

[42] "Understanding Review Types: Critical Reviews." [Online]. Available: https://libguides.lib.umanitoba.ca/reviewtypes/critical#:~:text=A%20critical%20review%20describes%20an,on%20the%20topic%20of%20review

[43] "The Critical Literature Review - Sociology." Harvard. Accessed: Jan. 05, 2023. [Online]. Available: https://sociology.fas.harvard.edu/files/sociology/files/literature_review.pdf

[44] M. J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, L. Shamseer, J. M. Tetzlaff, E. A. Akl, S. E. Brennan, R. Chou, J. Glanville, J. M. Grimshaw, A. Hróbjartsson, M. M. Lalu, T. Li, E. W. Loder, E. Mayo-Wilson, S. McDonald, L. A. McGuinness, L. A. Stewart, J. Thomas, A. C. Tricco, V. A. Welch, P. Whiting, D. Moher, "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," BMJ 2021; 372. https://doi.org/10.1136/bmj.n71

[45] I. Bongiovanni, "The Least Secure Places in the Universe? A Systematic Literature Review on Information Security Management in Higher Education," Computers & Security, vol. 86, 2019, pp. 350–357, https://doi.org/10.1016/j.cose.2019.07.003

[46] "PRISMA Flow Diagram." [Online]. Available: https://prisma-statement.org/prismastatement/flowdiagram.aspx

[47] M. N. AL-Nuaimi, "Human and Contextual Factors Influencing Cyber-Security in Organizations, and Implications for Higher Education Institutions: A Systematic Review," Glob. Knowl. Mem. Commun., 2022, https://doi.org/10.1108/GKMC-12-2021-0209

[48] A. Amigud, J. Arnedo-Moreno, T. Daradoumis, and A.-E. Guerrero-Roldan, "An Integrative Review of Security and Integrity Strategies in an Academic Environment: Current Understanding and Emerging Perspectives," Comput. Secur., vol. 76, pp. 50–70, 2018, https://doi.org/10.1016/j.cose.2018.02.021

[49] K. P. Patten and M. A. Harris, "The Need to Address Mobile Device Security in the Higher Education IT Curriculum," vol. 24, 2013.

[50] "AI and Machine Learnin in Cybersecurity - How They Will Shape the Future." Mar. 30, 2022. Accessed: Jan. 31, 2023. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/ai-cybersecurity

6 APPENDIX. LIST OF ELIGIBLE JOURNAL ARTICLES USED IN THE STUDY

Author and Year	Title
S. Faris, S. E. Hasnaoui, H. Medromi, H. Iguer, and A. Sayouti, (2014)	Information Security Policies: Investigation of Compliance in Universities
V. Singh and M. Margam (2018)	Information Security Measures of Libraries of Central Universities of Delhi: A Study
Z. Huang (2021)	An Analysis of Information Security and Protection Strategies in Colleges and Universities in the Environment of Smart Campuses
W. Gunawan (2005)	Measuring Information Security and Cybersecurity on Private Cloud Computing
Y. Xu (2013)	Research on Computer Network Security Architecture of Universities in China
C. Joshi and U. K. Singh (2017)	Information security risks management framework A step towards mitigating security risks in university network
Y. Zhao (2014)	Applied-Information Technology in the Internet of Things in the Construction of File Security System in Colleges and Universities
K. P. Patten and M. A. Harris (2013)	The Need to Address Mobile Device Security in the Higher Education IT Curriculum
A. Ghazvini, Z. Shukur, and Z. Hood (2018)	Review of Information Security Policy based on Content Coverage and Online Presentation in Higher Education
J. Merchan-Lima, F. Astudillo-Salinas, L. Tello-Oquendo, F. Sanchez, G. Lopez-Fonseca, and D. Quiroz (2021)	Information security management frameworks and strategies in higher education institutions: a systematic review
A. Amigud, J. Arnedo-Moreno, T. Daradoumis, and A.-E. Guerrero-Roldan (2018)	An integrative review of security and integrity strategies in an academic environment: Current understanding and emerging perspectives

7 AUTHORS

Miko Nuñez holds a Certified in Cybersecurity certification from the International Information Systems Security Certification Consortium and is pursuing CGRC and CISSP. He is currently a Cybersecurity Analyst for CyTech International. His experience covers incident response, risk management, governance, compliance, and

security operations. He has prior experience working in information security in the financial technology sector (email: miko.nunez@g.msuiit.edu.ph).

Xavier-Lewis Palmer, PhD, is an Engineer who focuses on technological intersections of Biocybersecurity. His prior degrees include two Master's degrees in Cybersecurity and Biotechnology and two Bachelor's degrees in Philosophy and Biology. His experience covers research, device design, device fabrication, data curation, and analysis, in addition to a variety of tissue engineering and biotechnological assays (email: xpalm001@odu.edu).

Lucas Potter earned his BS in Biomedical Engineering in 2015 from Virginia Commonwealth University and a PhD in Biomedical Engineering at Old Dominion University. He has researched human factors for three federal organizations and biomedical engineering for three private companies and is an active contributor to the field of biocybersecurity (email: lpott005@odu.edu).

Dr. Chris Jordan Aliac finished his bachelor's degree in Computer Engineering in 2002, Master's in Computer Science in 2004, and Doctor in Information Technology in 2015, all at Cebu Institute of Technology University. He is also a certified cloud practitioner by Amazon Web Service and a Certified Professional Computer Engineer by the Philippine Computer Engineering Certification Board. Dr. Aliac focuses his research on the fields of artificial intelligence, specializing in Robotics and Machine Learning, Embedded and Distributed Systems and ICT Security. Currently, He is the Manager for The CIT University's Makespace and CIT University ICT security Head. He is also a Full Professor at the College of Computer Studies in the same University (email: chris.aliac@cit.edu).

Lemuel Clark Velasco is an associate professor of information systems from the Department of Information Technology at the Mindanao State University Iligan Institute of Technology. He was the pioneering Director of FAB LAB Mindanao Center of Innovation and Invention, co-founder of FAB LABs Philippines-the Philippine FAB LAB Network, and co-founder of Webforest Digital Solutions. He is a predictive analytics researcher at the Premiere Research Institute of Science and Mathematics center for Computational Analytics and Modelling (email: lemuelclark.velasco@g.msuiit.edu.ph).