Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Cybersecurity Strategy for Higher Education Institutions: A Thematic Analysis on Standards and Frameworks

Milagros B. Barruga [1], Thelma D. Palaoag [2]
[1] *University of the Cordilleras, Baguio City, Philippines. Email: mbbarruga@mmsu.edu.ph*
[2] *University of the Cordilleras, Baguio City, Philippines. Email: tdpalaoag@uc-bcf.edu.ph*

ARTICLE INFO

Received: 20 Dec 2024

Revised: 12 Feb 2025

Accepted: 24 Feb 2025

ABSTRACT

Higher education institutions (HEIs) are increasingly vulnerable to cybersecurity attacks. As HEIs shift their operations online, they inevitably employ open systems and decentralized processing, making them particularly susceptible to cyberattacks. The study aims to identify the cybersecurity frameworks that HEIs currently employ as well as the characteristics that these frameworks must have. Initially, a comprehensive literature review was conducted to determine current cybersecurity practices and frameworks used by HEIs. This is followed by expert interviews with IT and cybersecurity professionals to gather insights into the attributes of effective cybersecurity frameworks. Qualitative data is analyzed through thematic coding to identify common characteristics and challenges. Finally, a proposed cybersecurity framework is developed by integrating these identified attributes with established cybersecurity concepts and best practices. The framework, developed from the identified attributes and established concepts, offers a comprehensive approach tailored to the specific needs of HEIs. By incorporating insights from industry professionals and aligning with best practices, the framework provides a robust tool for enhancing the cybersecurity posture of HEIs. This research contributes to the ongoing development of effective cybersecurity strategies in the higher education sector. It underscores the importance of a tailored approach to addressing the evolving cyber threat landscape.

Keywords: Cybersecurity framework, cybersecurity model, higher education institutions, thematic analysis.

INTRODUCTION

Academic organizations like higher education institutions (HEIs) are becoming more vulnerable to cyber-attacks, especially upon shifting from in-person to online teaching and learning. Universities are highly vulnerable to data breaches due to their complexity and dynamic digital environment [1]. To provide resources for teaching and learning, communication channels are open in design [2], [3], decentralized, and available for diverse types of users [3], [4], allowing for a network of multiple devices and diverse applications and technologies communicating in and out of the academic landscape.

HEIs also store large amounts of data on scientific works, ground-breaking research and innovation[3], intellectual property, and personal data about the researchers, faculty members, administrators, and staff members of support services, including personally identifiable information (PII) of the thousands of students. HEIs also keep other valuable assets including learning and teaching information, financial management information, administration details, and IT support services like bandwidth and internet connection, computing power and resources, and communication systems and data [5]. Moreover, some universities have outdated hardware and software, inadequate security policies and practices, a lack of cybersecurity expertise [6], and inadequate infrastructure [7]. These vulnerabilities attract threats and cyberattacks.

Threats are taking advantage of the unique characteristics of emerging technologies like social media, cloud computing, smartphone technology, and critical infrastructure, exploiting browser security, mobile malware, social engineering, botnets, and even inside knowledge and personnel [8]. The culture of collaboration and information

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

sharing in academic institutions is also a security challenge as it spreads the attack surface even wider [5]. Differing levels of online exposure, experience, and cybersecurity awareness while increasing access to cyber technologies make it more difficult to establish cybersecurity compliance [3]. Adhering to security protocols for higher education is also difficult due to the complexity and sometimes outdated operating systems and software [9].

HEIs are the target of cyberattacks in a variety of ways. Phishing, ransomware, DDoS, malware, direct-access or insider attacks, attacks against connected devices, and loss or theft of equipment are the most common types of cyberattacks in universities [10]. Unintentional disclosure is also evident [11]. Reported also are unauthorized access to the admissions database, university library patron database, graduate school applicants' records and alumni information; and data breach attacks on academic information (grade and in-state residency status of students) [9]. HEIs also become attractive targets of hackers as they often serve as hosts for critical infrastructure and user-intensive systems that are vital to the operation of a nation or city. These attacks not only negatively affect HEIs financially but their integrity and reputation are also challenged [12].

Data exposure risks and disruption to operations are minimized with appropriate security measures. These measures include employee training, safeguarding email communications, endpoint security, updating equipment, establishing and enacting cybersecurity policies, institutional device security, limited access to institutional devices, access management policy, and backup system [3], [10]. On the technical side, many institutions also adopted cloud computing services, compartmentalizing user privileges and account access, application controlling whitelisting, reviewing systems recovery plans, regular inventory of network devices, active and passive detection mechanisms, and utilizing application-aware network defenses [9]. Other cybersecurity technologies and practices are also recommended, including cloud vendor management (CVM), AI and Machine Learning, endpoint detection and response, single sign-on/multifactor authentication (SSO/MFA), preserving the authenticity and integrity of data, student data privacy and governance, behavior analytics, zero-trust model, data loss prevention, intrusion detection system/intrusion prevention system (IDS/IPS), security information and event management (SEIM), firewall, and antivirus[13].

The rapidly evolving landscape of cybersecurity necessitates a more holistic and integrated approach than merely implementing aggressive yet sporadic solutions. Some HEIs carried out comprehensive vulnerability assessments [7], introduced program logic models outlining roadmaps to mitigate cybersecurity threats [6], employed implementation frameworks to assess their security level, identify their weaknesses, determine the recommended mitigation plan [14] [15], and instituted mitigation controls and a system for continual review of information assets as per risk tolerances [16]. Due to persistent cyberattacks despite measures to mitigate them, some universities recognized the need to employ scientifically derived and actionable frameworks to develop cybersecurity programs [17]. These initiatives establish the rationale of HEIs in using a model that serves as a guide when planning and implementing cybersecurity strategies.

In the Philippines, the implementation of cybersecurity frameworks is primarily driven by the National Cybersecurity Plan 2023-2028 (NCSP). This plan is aligned with the broader goals of the Philippine Development Plan 2023-2028, the National Security Strategy, and the National Cybercrime Strategy. These strategies are aligned with the SDG9 goals of building resilient infrastructure, promoting inclusive and sustainable industrialization, and fostering innovation [25]. The NCSP aims to strengthen the country's cybersecurity capabilities through six key pillars, including policy improvements like the proposed Cybersecurity Act to enhance legal frameworks and organizational cybersecurity initiatives [26]. The cybersecurity framework of the National Institute for Standards and Technology (NIST CSF) provides guidelines and best practices to mitigate cyber risks and strengthen security postures, which could be relevant to institutions and organizations in the Philippines aiming to enhance their cybersecurity resilience [28].

This study explores the characteristics and attributes of a cybersecurity framework suitable for the unique needs of HEIs. The emphasis of this study is the thematic analysis of the gathered insights and recommendations of IT and cybersecurity professionals on the characteristics and attributes of cybersecurity frameworks that can be effective in addressing the unique challenges faced by these institutions in the Philippine setting. This study examines the experiences of Philippine HEIs in creating and executing cybersecurity plans, focusing on their perspectives on

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

framework adoption or standard compliance, the traits of successful cybersecurity frameworks, and the essential elements that must be included for them to be useful and efficient.

METHOD

The research employs a systematic thematic analysis process. Expert interviews were conducted with ten (10) IT professionals and cybersecurity specialists from state and local universities and colleges (SUCs and LUCs) to gain deeper insights into the institutional and technical requirements of cybersecurity framework development and implementation. The qualitative data allows for a more nuanced understanding of the strategic considerations, contextual factors, and best practices in cybersecurity management within HEIs. The results of this work are obtained using the six-step approach [28] to synthesize findings from guided interviews. The following steps were carried out: 1) transcription, familiarization with the data, and selection of quotations, 2) selection of keywords, 3) coding, 4) theme development, 5) conceptualization through interpretation of keywords, codes, and themes, and 6) final refinement and the development of the cybersecurity framework. This method works effectively for extracting themes that may be used as a guide to create concepts that form the foundation of a cybersecurity framework.

A semi-structured interview guide was utilized to gather participants' insights. Open-ended questions were asked on the following topics: a) characteristics of an effective cybersecurity framework, b) key components of a cybersecurity framework, and c) challenges in using a cybersecurity framework.

An interview guide was sent to the experts purposively selected as participants in the data-gathering exercise [29]. Follow-up interviews were carried out to validate their answers.

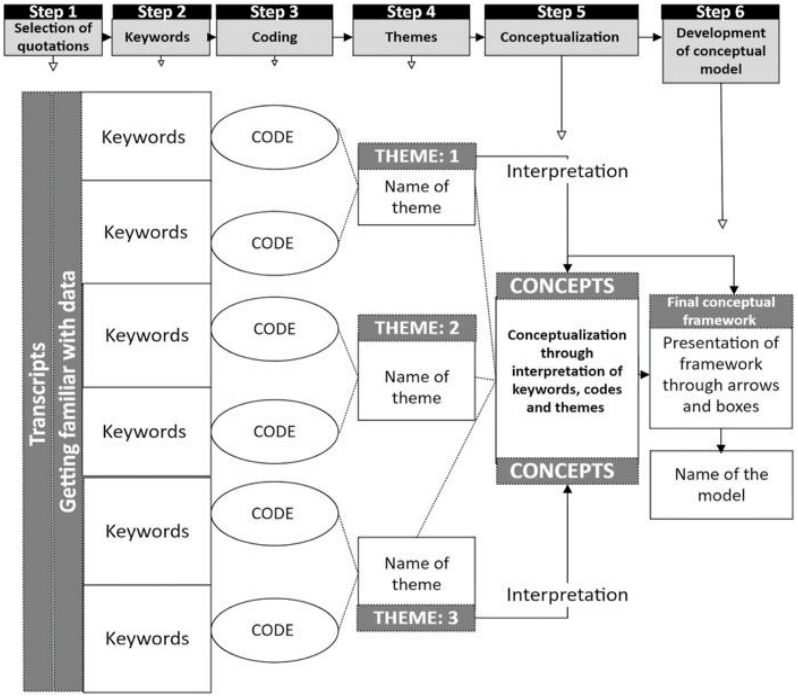

Fig. 1. The six-step approach

RESULTS AND DISCUSSION

Effective cybersecurity in HEIs requires a comprehensive, system-wide approach strategy that includes technical, administrative, and physical safeguards contextualized and dynamic to the unique characteristics of the HEI [18]. Implementing cybersecurity requires effective resource use, risk exposure identification, and communication between the technical team and upper management, all of which must be incorporated into university business plans and decision-making procedures [19]. Like in any organization, HEI's decision-makers consider relevant management success factors that directly impact the cybersecurity position of the organization [20].

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

HEIs may develop their guide, model, or framework of operation that is tailored to the peculiarities of their business goals and take into consideration their capacity and risk appetite. These mechanisms may also evolve and in some cases, recursively be upgraded to continue to be useful to cope with the changing needs of the organization [21]. Organizational learning frameworks can be established to develop countermeasure strategies in addressing cybersecurity challenges and improving digital resilience [22], [23]. A cybersecurity implementation framework proposes a set of adaptable security controls that oversee the implementation of cybersecurity strategies. It integrates high-level conceptual security controls, solutions, entities, tools, and techniques or mechanisms [24].

The insights gleaned from the participant responses in the data-gathering exercise highlight the level of awareness, involvement, and practices among IT professionals and faculty members in SUCs and LUCs. These insights are critical for understanding the current state of cybersecurity preparedness and informing the proposed framework. The study involved a diverse group of participants who assume varied roles in cybersecurity program implementation. This ensures a balanced perspective on cybersecurity practices in HEIs. Fifty percent (50%) of the participants are IT managers, and the others are faculty members specializing in IT. Ninety percent (90%) of the participants are from state universities and colleges (SUCs), and 10% are from local universities and colleges (LUCs). Sixty percent (60%) take active roles in cybersecurity program implementation in their respective institution.

All the participants are aware of the cybersecurity procedures that their organizations follow, even though some merely play a passive role in them. For example, the majority (80%) are aware that their institution implements some form of guidelines and policies for cybersecurity, 70% of them believe that their institution employs various technical controls such as encryption and secure protocols in data transmission and storage, 60% of them find the need to identify vulnerabilities, and 50% of them are aware that their institution has an incident response plan in place, which their institutions perform accordingly.

Concurrently, only two (2) are aware that their institution adopts a standard or framework in their cybersecurity program implementation. These two believe that the adoption of international standards and cybersecurity frameworks is construed as a key strategy for cybersecurity in their institutions. They claimed that their institution adopts well-established standards and frameworks. Although they were hesitant to talk about how they use the conventions of the guides, one complies with ISO 27001, and the other with NIST CSF. The others are not aware of any model, standard, or structure that they have created as a reference for implementing their cybersecurity program. However, each participant offered their perspectives on how frameworks could fit well in the HEIs' cybersecurity landscape.

A. Characteristics of an Effective Cybersecurity Framework

Table I presents the transcription of the captured data and the selected keywords derived through thematic analysis from the participants' answers about the characteristics of an effective cybersecurity framework. Each index number identifies distinct responses, with overlapping answers reflected by the absence of unique entries for all participants e.g. 9 entries for 10 participants indicate shared views.

Table I. Transcript and keywords for the characteristics of an effective cybersecurity framework

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Index	Characteristics of an effective cybersecurity framework	Keywords
1	Effective cybersecurity frameworks are comprehensive, adaptable, clear, and measurable, covering all aspects of an organization's digital environment while allowing for customization, easy implementation, and ongoing assessment of effectiveness.	comprehensive adaptable clear measurable covers all aspect of digital environment allows for customization easy implementation allows for ongoing assessment
2	It must be usable. An effective cybersecurity framework is one that is both robust enough to stop unauthorized network breaches and adaptable enough to let employees and partners get the data they need fast.	usable robust adaptable
3	Purposeful, Realistic and Achievable	purposeful realistic achievable
4	Cybersecurity in all aspects -stakeholders/end users, hardwares, network, etc	in all aspects
5	Processes of identifying the potential threats and protecting it.	identifies potential threat protect
6	Dedicated Cybersecurity Resources	dedicated resources
7	It's threat detection, prevention and response.	threat detection threat prevention response
8	The whole population should be involved in the deployment of cybersecurity framework.	whole population is involved
9	Not aware	not aware

The keywords were selected based on the 6Rs -realness, richness, repetition, rationale, repartee, and regal. These criteria ensured the keywords encapsulated the genuine experiences of the participants. The selected keywords offer a rich, insightful understanding of the participants' perspectives on cybersecurity practices and strategies, highlighting the practical and conceptual elements essential for effective cybersecurity frameworks.

Table II summarizes the thematic analysis results on coding and theme development. Codes are assigned for the keywords derived from the answers. Duplicate keywords were removed, and similar keywords were merged into a singular concept. Codes are assigned in a manner that can be categorized and analyzed for patterns and themes relating to the research questions. The codes were selected based on the 6Rs: robust, reflective, resplendent, relevant, radical, and righteous. Adhering to these criteria ensures that the assigned codes are robust enough to represent the keywords in a meaningful and comprehensive manner, encapsulating various aspects of cybersecurity frameworks. The code “holistic” is robust as it represents cybersecurity framework implementation to be “comprehensive” and “covers all aspects of the digital environment.” The keywords “allows for customization” and “realistic” as they relate to the HEIs’ existing capabilities, are appropriately coded as “flexible.” The analysis of the succeeding keywords went on with the same notions and conventions.

Table II. Coding and theming for the characteristics of an effective cybersecurity framework

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Keywords	Codes	Themes
comprehensive	holistic	integration of organizational culture integration of security technology
covers all aspect of digital environment		
adaptable	adaptable	flexibility and adaptability
allows for customization	flexible	
realistic		
easy implementation	simple	standardized practices
clear		
measurable	attainable	manageable (risk management approach)
achievable		
usable	functional	core functions and phases
robust	reliable	responsive (incident response procedures)
allows for ongoing assessment	continuous assessment	continuous improvement
purposeful	governed	security governance
has dedicated resources	allocated	

Themes were conceived by exploring the connections between the assigned codes – their similar meanings, shared context, or relationships, as they align well with the foundational concepts of cybersecurity frameworks [30].

Given this provision, the themes derived from the analysis realistically adhere to the 4Rs in theming: reciprocal, recognizable, responsive, and resourceful. There is certainly a mutual connection between the assigned codes and the themes. Themes closely align with the concepts of cybersecurity frameworks and directly address the requirements for developing a framework. For example, the code "holistic" mutually connects with the intrinsic characteristics of cybersecurity frameworks on the "integration of organizational culture" and integration of security technology." The assigned codes "adaptable" and "flexible" are generally taken as one as one of the intrinsic characteristics of the cybersecurity framework. Hence these codes are associates with the theme "flexibility and adaptability." The analysis went on for the succeeding keywords with the same notions and conventions for all the assigned codes.

The same procedures and observations were followed in the thematic analysis for the key components of a cybersecurity framework and the challenges in using it.

B. Key Components of a Cybersecurity Framework

Table III presents the transcription of data and selected keywords derived from the participants' answers to key components of a cybersecurity framework. Table IV presents the assigned codes and developed themes.

The keywords were grouped into related categories before coding to extract relevant codes. Then, the assigned code is aligned into themes through code associations. The keyword "threats" is coded as "risk" instead of a separate code. This is because threats can be considered one of the drivers of organizational risks, along with the organization's strengths, weaknesses, and opportunities. The keyword "AI integration" was initially coded as "controls". However, upon further investigation, AI can be integrated from end-to-end of the cybersecurity environment [31], and therefore, it is appropriately coded as a distinct keyword.

Table III. Transcript and keywords for the key components of a cybersecurity framework

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Index	Components of a cybersecurity framework	Keywords
1	1. Able to recognize the risks, weaknesses, threats, and assets 2. Capable of safeguarding secure settings, policies, and controls 3. Capable of detecting, tracking, recording, and responding to incidents 4. Capable of team response, communication, and recuperation	risks weaknesses threats assets secure settings policies controls incident management team response communication recuperation
2	An effective program must be comprehensive, or end to end, in scope—that is, the program must address all the critical elements that need to be protected in the institution.	critical elements
3	Policies and Guidelines, Physical Facilities and Security, Recovery Plan	policies and guidelines physical facilities and security recovery plan
4	AI integration	AI integration
5	risk management or mitigation	risk management risk mitigation
6	Policies and Procedures	policies procedures
7	The training and awareness of employees and Cyber Incident Response Plan	training of employees awareness of employees cyber incident response plan
8	The whole population should be involved in the deployment of cybersecurity framework.	whole population
9	Not aware	not aware

Each of the themes seems to be paralleled by the codes in Table IV. Since there are already themes that directly correspond with the codes, the codes in this instance cannot be further abstracted.

Table IV. Coding and theming for the key components of a cybersecurity framework

Keywords	Codes	Themes
risk	risk	risk assessment risk management
risk management		
risk mitigation		
threats		
assets (information assets)	asset	asset management
physical facilities and security		
critical elements		
secure setting	controls	access controls
controls		
policies	policies	information security policies
policies and guidelines		
procedures		
incidents	incident	incident management
incident response plan		
recovery plan	recovery	security assessment
recuperation		
training	training and awareness	awareness and training
awareness		
team response	users	communication
communication		
whole population		
AI integration	AI	AI integration

C. Challenges in using a Cybersecurity Framework

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table V presents the transcription of data and the derived keywords from the participant's answers to the challenges of using cybersecurity frameworks. It can be observed that several keywords were selected for the first entry in the summary table. These keywords are appropriate as each is rich in meaning and provide a detailed understanding of the characteristics of the cybersecurity frameworks that make them challenging to adopt or adhere to. Their meanings are distinct from each other and therefore, they must be taken separately as individual keywords apart from the other keywords identified by the participant. Table VI shows the assigned codes and themes, accordingly.

Table V. Transcript and keywords for challenges on the use of cybersecurity framework.

Index	Challenges on the use of cybersecurity framework	Keywords
1	challenges in complexity, resource limitations, infrastructure integration, user training, adapting to evolving threats, and meeting regulatory demands.	complexity resource limitations infrastructure integration user training adapting to evolving threats meeting regulatory demands
2	One significant challenge is the lack of cybersecurity awareness and training among employees.	lack of cybersecurity awareness and training
3	The ever changing patterns of attacks	ever changing patterns of attacks
4	Proper orientation and guidance in implementation	on the proper orientation and guidance in implementation
5	cyber security literacy	cbersecurity literacy
6	Budget Limitations and Talent Shortage	budget limitations talent shortage
7	The evolving cyberthreats	evolving cyberthreats
8	Compatability to the institution it would be deployed. e.g. culture, digital-divide	compatibilty to the institution culture digital-divide
9	Not aware	not aware

Table VI. Coding and theming for challenges on the use of cybersecurity framework.

Keywords	Codes	Themes
complexity	complexity	complexity
ever changing patterns of attacks		
evolving cyberthreats		
compatibilty to the institution		
lack of cybersecurity awareness and training	literacy	resistance form stakeholders
cbersecurity literacy		
on the proper orientation and guidance in implementation		
budget limitations	budget	inadequate resources

D. Conceptualization

The conceptualization process emanating from the analyzed data is anchored on the interconnection of elements in the information security ecosystem as outlined in the comprehensive model of management success factors (Fig. 2)

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

for information security decision-makers [20]. The themes derived from the characteristics, components, and challenges of the cybersecurity framework can be mapped into this model.

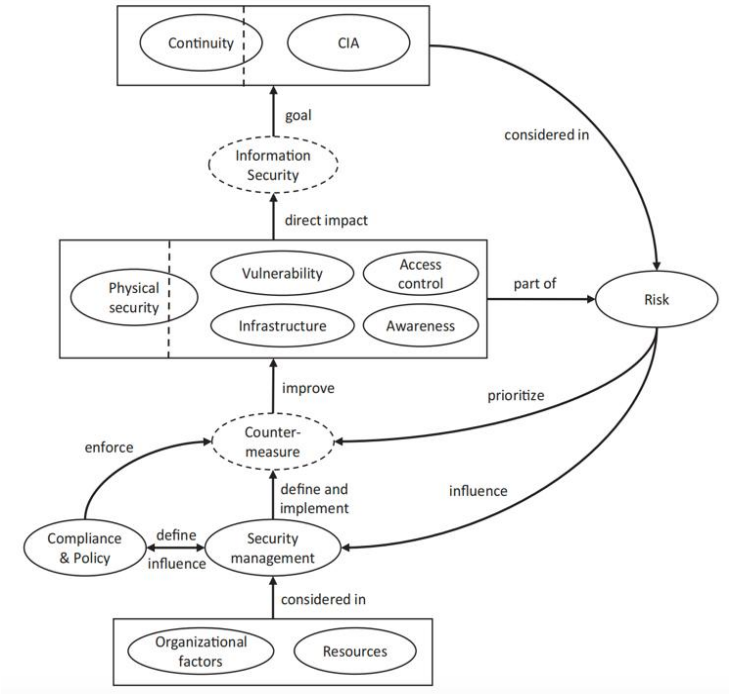

Fig. 2 A Comprehensive model of MSF

The use of a framework is a countermeasure strategy and a tool for security management. Therefore, to characterize the framework, one must probe the factors that affect the countermeasure or security management, in this case, the risk and organizational factors and resources. Risk is the possible occurrence of threats, organizational factors are properties of the organization, and resources include budget and the availability of good, skilled employees. An effective cybersecurity framework must entail a robust security measure to combat escalating cyber risks. It should also be flexible and adaptable and can be tailored for managing cyber risks in various organizational contexts, including the financial capability of the HEI. It should also entail resiliency, that is, implementing proactive measures to enhance cybersecurity posture. The framework must also usher in the implementation of cybersecurity practices that are aligned with organizational objectives and project goals, integrating technology and information security, and compliance with policies and adherence to governance.

In cognizance, the derived themes from the analysis are in synch with these expected characteristics: integration of organizational culture and integration of security technology, flexibility and adaptability, standardized practices (adherence to governance), risk management approach, core functions and phases (robust), incident response procedures (resilient), continuous improvement (flexibility and adaptability), and security governance (adherence to governance). Except for budgetary constraints, all the derived themes are incongruent with the MSF model.

The themes derived from analysis, as regards key components of a cybersecurity framework, can also be construed using the summary of framework components [32] but only to those that apply to HEIs. These include information security policies, asset management, access control, business continuity plan, compliance, incident management, risk assessment, security assessment, awareness and training, governance, data security, communication, analysis, and recovery plan. Of the themes conceived from the analysis, only AI integration is not evident in the desired components. The recency of AI could explain the apparent nonexistence.

As regards the challenges in the use of cybersecurity frameworks, the association of factors in the MSF model (Fig. 2) could set the criteria for determining them. Cybersecurity frameworks as countermeasures or tools for security management are affected by the prioritization and nature of threats, the consideration of organizational factors, and the availability of resources.

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The themes developed from the analysis identify complexity, resistance of stakeholders, and inadequate resources. Complexity can encompass the changing nature of threats of attack. Resistance of stakeholders may emanate from top management who do not recognize the gravity of the threat, regular employees who are oblivious of the impact of cyber-attacks, or simply an issue of prioritizing resources due to lack of communication.

E. Development of the cybersecurity model

The developed themes can be illustrated fairly in Fig. 3. The themes for the characteristics of effective cybersecurity framework were reworded as adjectives instead of nouns, as they should describe or characterize the framework. For example, the theme "flexibility and adaptability" is reworded as "flexible and adaptable". Also, from "integration" to "integrated approach", from "standardized practices" to "standardized", from "core functions and phases" to "robust", from "continuous improvement" to "dynamic", and from "security governance" to "compliant".

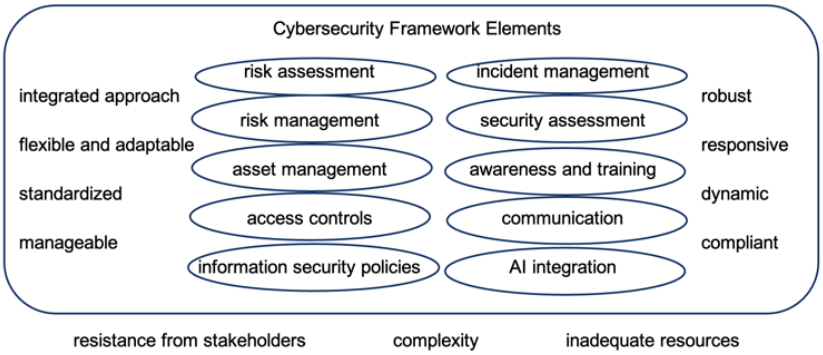

Fig. 3 Conceptual Model of the Cybersecurity Framework

In Fig. 3, the elements enclosed in oblong inside the rounded box are the framework's components. The elements surrounding the enclosed components are the themes that characterize the framework, thereby surrounding the components. Then, the elements below and outside the rounded box are the challenges in using the framework. They are outside the rounded box because these elements represent the challenges that may hamper the implementation of cybersecurity programs.

The conceptual model can be further enhanced by incorporating the concepts of shared actions, cybersecurity pillars, and the framework life cycle [33]. Shared actions outline common activities in the cybersecurity program implementation. Cybersecurity pillars are the aspects of the institution that need to be strengthened with cybersecurity. The framework life cycle provides a structured approach to security.

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

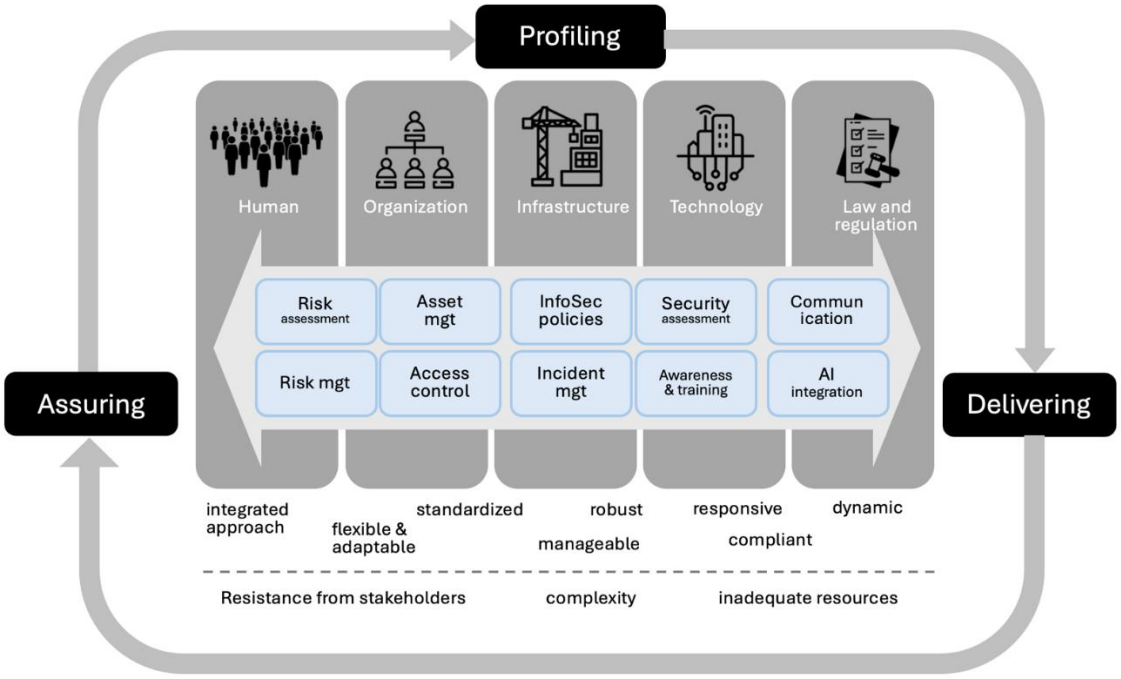

Fig. 4 Proposed Cybersecurity Framework

Fig. 4 illustrates the proposed cybersecurity framework, highlighting the shared actions, pillars, and life cycle. The shared actions, being the common activities in cybersecurity, are the ten (10) developed themes derived from the thematic analysis. The themes were translated as the shared actions in the framework development. The shared actions cut across the five pillars of cybersecurity, as depicted by the two-sided arrows enclosing them. This entails that the operations of any of the shared actions affect the five aspects of the institution - aspects in human, organization, technology, infrastructure, and law and regulation in one way or another.

The operations of the shared actions must satisfy certain levels of effectiveness. The criteria for effectiveness were the derived themes from the thematic analysis of the characteristics of an effective cybersecurity framework. The characteristics expressed in the investigation were translated as criteria for evaluating the effectiveness of executing any shared actions in the framework. This entails that to ensure effective protection, the execution of cybersecurity implementation must conform to the defined set of criteria of operation.

To sustain effective security and protection, the implementation and operation of the framework should be consistent throughout the framework lifecycle – from profiling to delivering through assuring, and back to profiling.

CONCLUSION

The thematic analysis on the use of standards and framework provides baseline information for developing a novel cybersecurity framework tailored to the peculiar needs and requirements of Philippine HEI. Ten (10) IT experts and cybersecurity professionals participated in the investigation by answering a semi-structured interview guide and sharing their insights on the characteristics and key components of an effective cybersecurity framework. Through thematic analysis, themes were derived and later translated as elements of the novel framework. The insights elicited from the investigation serve as valid references to the actual and current needs and requirements of the HEIs. Aligning these findings with established underpinnings of cybersecurity ensures that the elements in the proposed framework are a robust tool for enhancing the cybersecurity posture of HEIs. This research contributes to the ongoing development of effective cybersecurity strategies in the higher education sector. It underscores the importance of a tailored approach to addressing the evolving cyber threat. The framework is a living document. The components and features of which can vary over time due to the dynamic nature of technology, especially cybersecurity. Listening from other experts including professionals from private and other government schools could enhance further the

Research Article

features that were initially included in the framework. More inputs could reveal fresh insights that corroborate the findings of this work. Until new inputs are at bay, IT managers and cybersecurity officers in the Philippine HEIs can employ this new framework as a reference in their operational and strategy planning for cybersecurity program implementation.

REFERENCES

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

[2] C. L. Borgman, "Open Data, Grey Data, and Stewardship: Universities at the Privacy Frontier," 2018, doi: 10.15779/Z38B56D489.

[3] S. Yusif and A. Hafeez-Baig, "Cybersecurity Policy Compliance in Higher Education: A Theoretical Framework," *J. Appl. Secur. Res.*, vol. 18, no. 2, pp. 267–288, Apr. 2023, doi: 10.1080/19361610.2021.1989271.

[4] K. A. Yousif Yaseen, "Importance of Cybersecurity in The Higher Education Sector 2022," *Asian J. Comput. Sci. Technol.*, vol. 11, no. 2, pp. 20–24, Dec. 2022, doi: 10.51983/ajcst-2022.11.2.3448.

[5] J. B. Ulven and G. Wangen, "A Systematic Review of Cybersecurity Risks in Higher Education," *Future Internet*, vol. 13, no. 2, p. 39, Feb. 2021, doi: 10.3390/fi13020039.

[6] N. M. De Ramos and F. D. Esponilla Ii, "Cybersecurity program for Philippine higher education institutions: A multiple-case study," *Int. J. Eval. Res. Educ. IJERE*, vol. 11, no. 3, p. 1198, Sep. 2022, doi: 10.11591/ijere.v11i3.22863.

[7] M. A. E. Telen, P. T. Abamonga, and T. P. Chua, "MITIGATING CYBER THREATS TO PHILIPPINE STATE UNIVERSITIES AND COLLEGES: A COMPREHENSIVE VULNERABILITY ASSESSMENT OF UNIVERSITY OF SCIENCE AND TECHNOLOGY OF SOUTHERN PHILIPPINES - CAGAYAN DE ORO CAMPUS ICT INFRASTRUCTURES".

[8] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *J. Comput. Syst. Sci.*, vol. 80, no. 5, pp. 973–993, Aug. 2014, doi: 10.1016/j.jcss.2014.02.005.

[9] George Liluashvili, "Cyber Risk Mitigation in Higher Education," *Int. J. Law*, vol. 7, no. 2, pp. 15–27, Apr. 2021, doi: 10.36575/7.2.2.

[10] M. A. Haque *et al.*, "Cybersecurity in Universities: An Evaluation Model," *SN Comput. Sci.*, vol. 4, no. 5, p. 569, Jul. 2023, doi: 10.1007/s42979-023-01984-x.

[11] L. Coleman and B. M. Purcell, "Data Breaches in Higher Education," vol. 15, 2015.

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

[13] A. B. Nassoura, "Cybersecurity Technologies And Practices In Higher Education Institutions: A Systematic Review," vol. 19, no. 3, 2022.

[14] B. M. Dioubate, W. Daud, and W. Norhayate, "Cyber Security Risk Management Frameworks Implementation in Malaysian Higher Education Institutions," *Int. J. Acad. Res. Bus. Soc. Sci.*, vol. 12, no. 4, p. Pages 1356-1371, Apr. 2022, doi: 10.6007/IJARBSS/v12-i4/12300.

[15] I. Almomani, M. Ahmed, and L. Maglaras, "Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia," *PeerJ Comput. Sci.*, vol. 7, p. e703, Sep. 2021, doi: 10.7717/peerj-cs.703.

[16] Mr. P. Macharia Njoroge, "An Examination of Threats facing Assets in Use in Kenyan Public Universities," *Int. J. Sci. Res. Publ. IJSRP*, vol. 11, no. 5, pp. 687–695, Apr. 2021, doi: 10.29322/IJSRP.11.05.2021.p11372.

[17] B. Badamasi and S. C. A. Utulu, "FRAMEWORK FOR MANAGING CYBERCRIME RISKS IN NIGERIAN UNIVERSITIES," 2021.

[18] E. C. K. Cheng and T. Wang, "Institutional Strategies for Cybersecurity in Higher Education Institutions," *Information*, vol. 13, no. 4, p. 192, Apr. 2022, doi: 10.3390/info13040192.

[19] "The Role of Cybersecurity on the Performance of Malaysian Higher Education Institutions," *J. Pengur.*, vol. 67, Mar. 2023, doi: 10.17576/pengurusan-2023-67-03.

[20] R. Diesch, M. Pfaff, and H. Krcmar, "A comprehensive model of information security factors for decision-makers," *Comput. Secur.*, vol. 92, p. 101747, May 2020, doi: 10.1016/j.cose.2020.101747.

Research Article

[21] H. Taherdoost, "Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview," *Electronics*, vol. 11, no. 14, p. 2181, Jul. 2022, doi: 10.3390/electronics11142181.
[22] S. Mahmood, M. Chadhar, and S. Firmin, "Digital resilience framework for managing crisis: A qualitative study in the higher education and research sector," *J. Contingencies Crisis Manag.*, vol. 32, no. 1, p. e12549, Mar. 2024, doi: 10.1111/1468-5973.12549.
[23] S. Mahmood, M. Chadhar, and S. Firmin, "Countermeasure Strategies to Address Cybersecurity Challenges Amidst Major Crises in the Higher Education and Research Sector: An Organisational Learning Perspective," *Information*, vol. 15, no. 2, p. 106, Feb. 2024, doi: 10.3390/info15020106.
[24] I. Atoum and A. Otoom, "A Classification Scheme for Cybersecurity Models," *Int. J. Secur. Its Appl.*, vol. 11, no. 1, pp. 109–120, Jan. 2017, doi: 10.14257/ijsia.2017.11.1.10.
[25] "Cyber Peace & the Sustainable Development Goals (SDGs)."
[26] *National Cybersecurity Plan 2023-2028*, Feb. 2024. [Online]. Available: https://dict.gov.ph/national-cybersecurity-plan-2023/
[27] G. M. Nist, "The NIST Cybersecurity Framework 2.0," National Institute of Standards and Technology, Gaithersburg, MD, NIST CSWP 29, 2023. doi: 10.6028/NIST.CSWP.29.
[28] M. Naeem, W. Ozuem, K. Howell, and S. Ranfagni, "A Step-by-Step Process of Thematic Analysis to Develop a Conceptual Model in Qualitative Research," *Int. J. Qual. Methods*, vol. 22, p. 16094069231205789, Oct. 2023, doi: 10.1177/16094069231205789.
[29] I. Etikan, "Comparison of Convenience Sampling and Purposive Sampling," *Am. J. Theor. Appl. Stat.*, vol. 5, no. 1, p. 1, 2016, doi: 10.11648/j.ajtas.20160501.11.
[30] M. Barruga, "Cybersecurity Strategy for Higher Education Institutions: A Systematic Review," *Unpublished*.
[31] S. Zeadally, E. Adi, Z. Baig, and I. A. Khan, "Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity," *IEEE Access*, vol. 8, pp. 23817–23837, 2020, doi: 10.1109/ACCESS.2020.2968045.
[32] M. Syafrizal, S. R. Selamat, and N. A. Zakaria, "Analysis of Cybersecurity Standard and Framework Components," *Int. J. Commun. Netw. Inf. Secur. IJCNIS*, vol. 12, no. 3, Apr. 2022, doi: 10.17762/ijcnis.v12i3.4817.
[33] R. Azmi, W. Tibben, and K. T. Win, "Review of cybersecurity frameworks: context and shared concepts," *J. Cyber Policy*, vol. 3, no. 2, pp. 258–283, May 2018, doi: 10.1080/23738871.2018.1520271.