Towards a Tailored Cybersecurity Education Framework for Malaysia: A Systematic Literature Review

Muhammad Asfand Yar[1], Hock Guan Goh[2], Kiran Adnan[3], Ming Lee Gan[4], Vasaki Ponnusamy[5]
Faculty of Information and Communication Technology (FICT),
Universiti Tunku Abdul Rahman (UTAR), Kampar, Malaysia[1,2,3,4]
Higher Colleges of Technology, United Arab Emirates, Saudi Arabia[5]

***Abstract*—Developing countries including Malaysia faces urgent challenges in cybersecurity education: preparing graduates who meet industry demands while addressing national cultural and regulatory contexts. Despite global advancements, no localized education framework currently aligns Malaysian higher education curricula with industry-required competencies. This systematic literature review (SLR) analyzed 65 academic and gray literature sources selected from an initial pool of 706 studies. The review employed thematic synthesis to examine the Malaysian cybersecurity programs incorporate technical competencies, policy literacy, and contextual relevance. Findings reveal four recurring gaps: limited integration of industry-aligned technical skills, insufficient adoption of hands-on pedagogies such as labs and gamification, underrecognition of professional certifications, and minimal incorporation of local policy and cultural considerations. These insights emphasize the necessity of a context-aware cybersecurity education framework tailored for Malaysia. The study provides a conceptual foundation for designing an industry-driven curriculum model, supporting future research on cybersecurity competency development in higher education.**

***Keywords*—Cybersecurity education; systematic literature review; Malaysia; industry competencies; higher education; curriculum model; hands-on learning**

LIST OF ABBREVIATIONS

Abbreviation	Nomenclature
QA	Quality Assurance
NIST	National Institute of Standards and Technology
CISSP	Certified Information Systems Security Professional
CTF	Capture The Flag
COBIT	Control Objectives for Information and Related Technologies
SLR	Systematic Literature Review
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
GIAC	Global Information Assurance Certification
ISACA	Information Systems Audit and Control Association
CISM	Certified Information Security Manager
NACSA	National Cyber Security Agency
NICE	National Initiative for Cybersecurity Education
CompTIA+	Computing Technology Industry Association
CEH	Certified Ethical Hacker
ISO	International Organization for Standardization
PICOC	Population, Intervention, Comparator, Outcome, Context
ISC2	International Information Systems Security Certification Consortium
EC-Council	International Council of E-Commerce Consultants
PDPA	Personal Data Protection Act
VR/AR	Virtual Reality / Augmented Reality

I. INTRODUCTION

Cybersecurity has become an important aspect of national resilience. Education serves as the strategic aspect to nourish a skilled and sustainable workforce. As cyber threats continue to be a major hurdle, there is a need for professionals who possess both technical proficiency and contextual understanding. In this regard, higher education institutions play an impotent role in developing this talent. It ensures not only technically capable workforce but also aware of regulatory frameworks, ethical considerations, and cultural contexts.

For the purpose of this study, cybersecurity is defined as the collection of technologies, processes, competencies, and governance practices that protect digital systems, networks, and data from threats, while ensuring confidentiality, integrity, availability, and regulatory compliance. This definition aligns with international perspectives (e.g., NICE, CyBOK) but is adapted to emphasize competencies and contextual factors relevant to Malaysia's educational and regulatory environment.

Universities and training institutions over the globe are searching for modern solutions to the existing challenges in the field of cybersecurity. New techniques such as, simulation labs and capture the flag competitions, are emerging as practical solutions to the complex cybersecurity problems [1], [2]. Similarly, professional certifications like CISSP and CEH have also been viable options to enhance employment and align curricula with evolving industry standards [3], [4]. Although these emerging practices are providing a basic framework, their direct adoption without contextual adaptation may not effectively serve national priorities.

In developing countries, cybersecurity remains a constant challenge. In particular, Malaysia is rapidly embracing digital economy. The growing reliance on technology-driven services demand a skillful cybersecurity workforce. Yet, the global curricula guidelines remain alien to the local regulations, cultural, and operational context. Studies illustrates that global cybersecurity standards like, COBIT and ISO 27001, for Malaysian institutions are helpful, though a comprehencive cybersecurity education framework still remains absent [5], [6].

The current studies are mainly focus on technical skills, hands-on learning, or certification alignment individually. There is still a scarcity of studies which unifies these components into a context-aware model. The lack of such a framework remains a hurdle both curriculum modernization and the

industry's ability to access competent graduates. Addressing this gap requires a thorough examination of the contemporary cybersecurity programs of Malaysia, which will not only cope with industrial needs but also evolve through a localized educational framework.

The next section outlines the research methodology, detailing how studies were identified, screened, and evaluated using the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines. This structured process ensures that the review findings are comprehensive, replicable, and directly aligned with the research objectives and questions presented above. Section IV presents the results and findings. Section V discusses the implications of these findings, while Section VI concludes the paper and outlines directions for future research. Section VII provides author declarations. References are listed at the end of the paper.

II. Related Works

A comprehensive review of the literature indicates emphasis on structured cybersecurity education. The specific areas targeted within the field are guidance to design a curriculum suitable for skills development. This section analyzes the existing research in cybersecurity education around the globe with a specific focus on Malaysia, which will help to locate the gaps, leading to the development of a Malaysian cybersecurity education framework.

A. Global Cybersecurity Education Frameworks

The literature suggests some benchmarks worldwide for curriculum development and professional certification. One of them is National Initiative for Cybersecurity Education (NICE) which is used as a standard structured guidelines for developing cybersecurity roles, tasks, and competencies prevalent across the globe [7]. This framework has been influential in shaping curriculum and cybersecurity training through scenario-based learning and cyber range implementations. Similarly, another framework, the Cyber Security Body of Knowledge (CyBOK), offers a comprehensive taxonomy of cybersecurity knowledge areas spanning software security, human factors, and systems security [8]. However, their direct adoption without contextual adaptation may not fully address the unique regulatory and cultural considerations in countries like Malaysia.

B. Cybersecurity Education in Malaysia

In Malaysia, studies suggest a growing integration of cybersecurity subjects and hands-on learning strategies within higher education institutions [9]. Risk management frameworks used in Malaysian universities, however, are still evolving and often lack comprehensive institutional maturity [10]. likewise, efforts toward localizing professional competency examinations are also underway, with frameworks being proposed to enhance certification for cybersecurity professionals [11]. Meanwhile, awareness initiatives have contributed to positive behavior change in Malaysian youth, yet sustained improvements require curriculum realignment and strengthened implementation of national policies [12]. Moreover, recent research highlights that students' cybersecurity behavior is influenced by cognitive and environmental factors, underscoring the need for a more contextualized educational approach [13].

C. Identified Gaps in Current Cybersecurity Education

Despite advancements, the literature still identifies notable gaps in current Malaysian cybersecurity education. It includes a poor integration of industry-aligned technical skills and hands-on engagement. Additionally, the contemporary frameworks also did not cope well with respect to national regulatory framework and local cultural factors [10]. These gaps remain a hurdle in ingraining technical expertise and contextual understanding in the Malaysian graduates in cybersecurity education. This review highlights the need for a local cybersecurity education framework informed by global best practices and aligned with Malaysia's national priorities.

III. Method

The multidisciplinary nature of cybersecurity education research requires a structured review. Thus, the study is conducted through the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework. It provides clear guidelines for identifying, assessing, and synthesizing literature from the relevant resources, as depicted in Fig. 1 [14].

The review process was organized into three key phases: selection and identification, evaluation, and synthesis. During the selection phase, two primary sources of literature were examined: the first one is academic databases such as IEEE Xplore, ACM Digital Library, and Scopus, and Google web-based searching was used as a second source to identify gray literature. The inclusion of gray literature enabled the review to capture materials not indexed in academic databases. The combination of academic and gray literature sources was considered sufficient to achieve comprehensive coverage and meet the objectives of this review.

The review process began with an initial pool of 706 records from academic litereature and 12 from other sources , from which 260 were removed before screening. 289 articles were excluded based on title and abstract screening. 157+12=169 records sought for retrieval, only 100+8 found eligible. Based on relevance, scope, and quality criteria, 40+3 studies were excluded. Consequently, 65 studies met all inclusion requirements and were synthesized in this review. Fig. 1 and the following sections provides a comprehensive summary of the study.

A. Selection and Identification

The search strategy was formulated to identify studies related to cybersecurity educational frameworks within Malaysian higher education institutions. Table I illustrates the keywords used to retrieve publications from each database. Extensive search was conducted to cover relevant studies published between 2010 and 2025, which resulted in academic and gray literature.

1) Academic literature search: The search strategies combined keywords to form strings for capturing sufficient information for a comprehensive study [15]. The distribution of records retrieved from various databases is presented in Fig. 2. The bar chart provides a more detailed preview of the studies across different databases. Among them, Google Scholar covered a large portion of academic literature. Although the more specialized sources provided fewer studies, the contribution resulted in a comprehensive and valuable addition to the study.

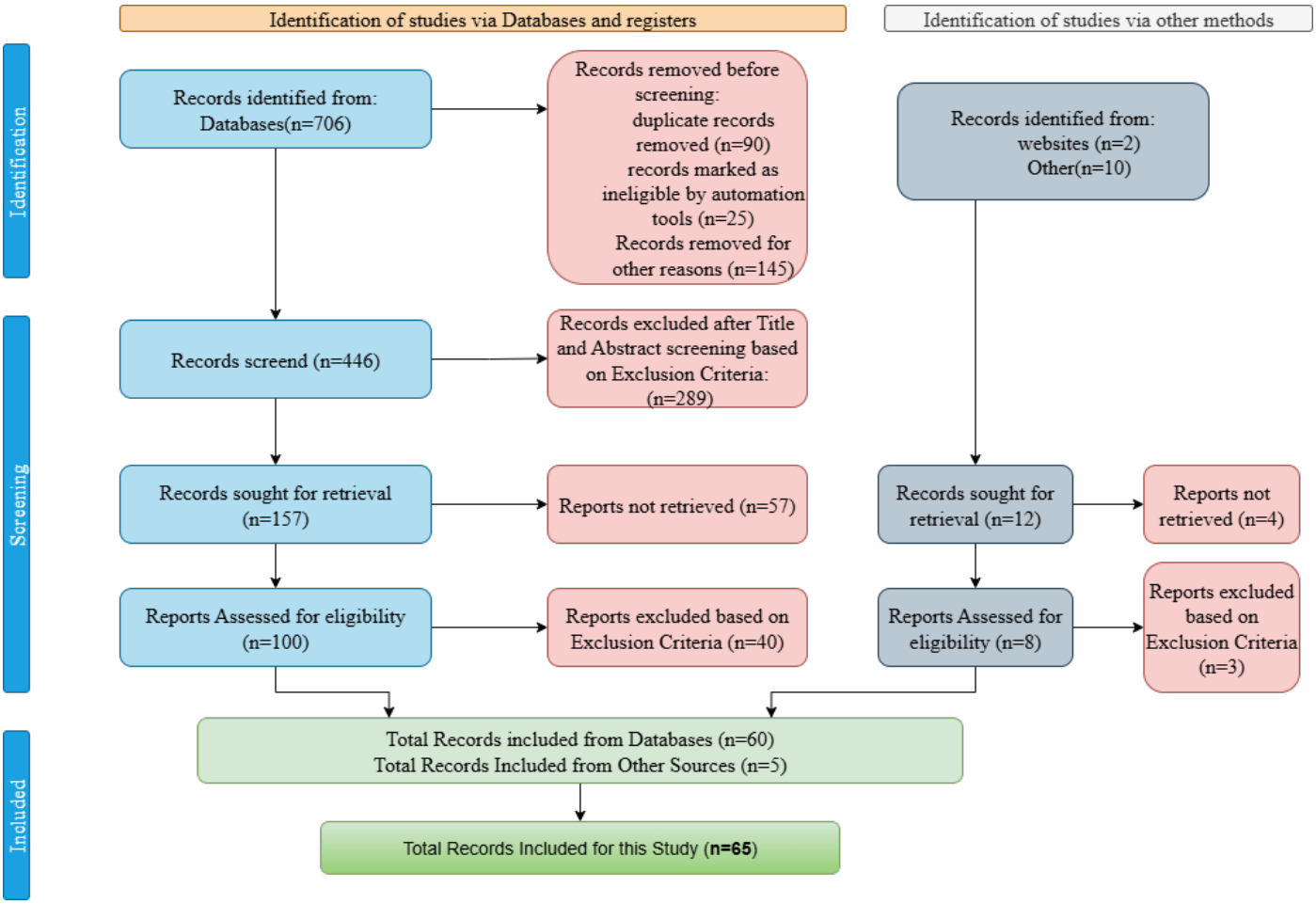

Fig. 1. PRISMA flowchart adapted from study [14].

TABLE I. KEYWORDS USED IN THE DATABASE SEARCH AND THEIR RELEVANCE

Keyword(s)	Description
cyber security OR cybersecurity OR information security	Covers literature related to protecting information systems, networks, and data from cyber threats. Variations of the term ensure comprehensive coverage of the cybersecurity domain.
education OR curriculum	Targets studies addressing the educational dimension of cybersecurity, including teaching methods, learning environments, and course content design.
framework	Identifies studies discussing models or structures for organizing cybersecurity education and competencies.
higher education	Narrows the search to post-secondary institutions such as universities and colleges, focusing on programs at the bachelor's level or higher.
industry requirements OR industry collaboration	Captures literature on how cybersecurity education aligns with industry standards, skill demands, and collaborative initiatives between academia and industry.
Malaysia OR Southeast Asia OR developing countries	Focuses on regional and socioeconomic contexts relevant to Malaysia and comparable settings, retrieving studies that reflect local regulations, challenges, and industry needs.

2) Other methods (gray literature): Similarly, the inclusion of gray literature is also necessary for a detailed overview of the present state of the topic under review. Therefore, the same databases, Scoopus and google scholar were used to search for a wider reange of keywords. Cybersecurity and information security related to higher education and industry standers

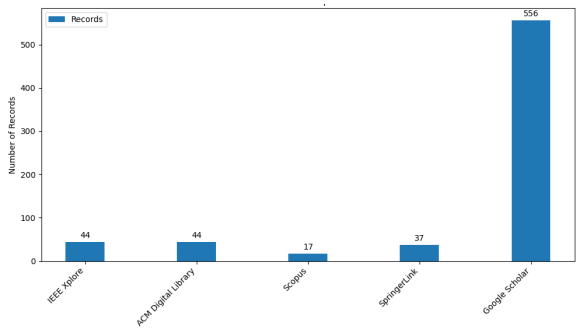

Fig. 2. Distribution of retrieved records across academic databases: Bar chart showing the number of records per database.

within Malaysia were considered. To mitigate the limitations of predefined keywords, faceted searches incorporating synonyms and alternative terminology were implemented, minimizing the risk of omitting relevant studies. In addition, the reference lists of key publications were manually examined to identify further studies related to cybersecurity education frameworks, industry requirements, and regional influences.

These combined strategies yielded twelve records from the gray literature, two from websites and ten from other

TABLE II. EVALUATION CRITERIA INCLUDING INCLUSION AND EXCLUSION CRITERIA

Protocol	Criteria
Interval	2010–2025
Inclusion Criteria	• Studies focusing on cybersecurity education frameworks within Malaysian higher education institutions. • Publications discussing integration of technical skills, policy understanding, industry collaboration, and cultural considerations in educational frameworks. • Articles published in peer-reviewed journals, conference proceedings, and relevant academic outlets.
Exclusion Criteria	• Studies focusing solely on general cybersecurity education without a framework-specific approach. • Papers that do not directly address the Malaysian context or lack insights into localized adaptations or implementations. • Publications outside the specified date range. • Studies not written in English.

TABLE III. QUALITY ASSESSMENT CRITERIA FOR SELECTION OF RELEVANT PAPERS

Criteria	Code	Description	Weight
Relevance	(QA1)	Does the study focus on cybersecurity education frameworks?	25%
Methodology	(QA2)	Is the research methodology robust and well-defined?	30%
Industry Focus	(QA3)	Does the paper discuss industry standards or requirements?	20%
Local Context	(QA4)	Does the study address regulations or cultural factors in cybersecurity education?	25%

non-indexed sources. furthermore, no additional entries were retrieved from citation tracking or organizational databases. This integrative and context-sensitive approach ensured the inclusion of diverse and regionally relevant perspectives within the review.

B. Evaluation

The study selection and evaluation process followed the PRISMA guidelines, as illustrated in Fig. 1. In total, six inclusion and three exclusion criteria were established to guide the final selection, as summarized in Table II.

1) Quality assessment: The quality of the selected studies was evaluated through predefined criteria. It encompassing relevance to the research objectives,, alignment with industry needs, and consideration of policy and regulatory factors within the Malaysian context. This systematic quality appraisal resulted in inclusion of credible and contextually significant studies only. The detailed assessment criteria applied during this process are summarized in Table III.

2) Assigning weights to the articles: To prioritize studies based on their methodological quality and contextual relevance, a weighted scoring system was applied to evaluate all selected studies. Predefined quality assessment (QA) criteria guided this process, with each study assessed against four QA dimensions and assigned a score reflecting its level of compliance with each criterion. The final weights were calculated proportionally to these scores, ensuring that studies demonstrating higher methodological rigor and contextual relevance were given greater significance in the synthesis [16].

a) Scoring system: Each quality assessment criterion was evaluated on a three-point scale as follows:

leftmargin=*

- 0 = Not addressed,
- 1 = Partially addressed or unclear,
- 2 = Fully addressed and well explained.

b) Category weighting: The quality assessment questions were categorized based on their relevance to the research objectives, and each category was assigned a weight corresponding to its importance within the overall evaluation framework.

c) Inclusion threshold: To maintain analytical rigor, a minimum threshold of 50% of the total possible score was established. Studies scoring below this threshold were excluded to ensure that only high-quality and contextually relevant articles were included in the final synthesis.

d) Calculation process: To calculate the overall quality score for each article, a weighted scoring method was applied. Each quality assessment criterion (e.g., relevance, methodology, industry focus, and local context) was assigned a weight based on its relative importance. The total score was derived as the sum of the weighted scores across all criteria, as shown in Eq. (1):

$$\text{Score} = \sum_{i=1}^{n} (w_i \times s_i) \tag{1}$$

where w_i represents the weight assigned to the i^{th} criterion, s_i is the score for the i^{th} criterion, and n is the total number of criteria under evaluation.

3) Quality assessment of studies: The studies that satisfied the inclusion threshold described in Section III-B2c were considered for the final review. Each study was evaluated based on the QA criteria outlined in Section III-B2, with scores assigned according to the system described in Section III-B2a. Final scores were then computed using the weighting and calculation procedures detailed in Sections III-B2b and III-B2d, respectively. Only studies that met the required threshold are presented in Table IV.

C. Synthesis

To enable a comprehensive comparison of the results across the reviewed studies, key categories of information were identified to guide the analysis and synthesis of findings. Given the research focus on cybersecurity education frameworks within the Malaysian context, the critical categories extracted include:

- Cybersecurity framework development in Malaysian higher education
- International standards and local adaptation
- Professional certifications and industry alignment
- Hands-on learning and experiential education

TABLE IV. QUALITY ASSESSMENTS OF STUDIES CONSIDERED FOR INCLUSION

Study	Reference	QA1	QA2	QA3	QA4	Score
S-1	[2]	2	2	2	2	2.00
S-2	[17]	2	2	2	2	2.00
S-3	[5]	1	2	2	2	1.75
S-4	[18]	2	2	2	1	1.75
S-5	[4]	1	2	2	2	1.75
S-6	[19]	1	2	2	2	1.75
S-7	[20]	2	1	2	2	1.70
S-8	[21]	2	1	2	2	1.70
S-9	[1]	2	2	0	2	1.60
S-10	[22]	1	2	1	2	1.55
S-11	[23]	1	2	1	2	1.55
S-12	[24]	1	2	1	2	1.55
S-13	[25]	2	2	1	1	1.55
S-14	[3]	1	2	1	2	1.55
S-15	[26]	2	2	2	0	1.50
S-16	[27]	1	2	2	1	1.50
S-17	[28]	2	2	2	0	1.50
S-18	[29]	2	2	2	0	1.50
S-19	[30]	2	2	2	0	1.50
S-20	[31]	2	2	2	0	1.50
S-21	[32]	2	1	2	1	1.45
S-22	[33]	2	1	2	1	1.45
S-23	[34]	2	1	2	1	1.45
S-24	[35]	1	1	2	2	1.45
S-25	[36]	1	1	2	2	1.45
S-26	[37]	1	2	1	1	1.30
S-27	[38]	2	2	1	0	1.30
S-28	[39]	2	2	1	0	1.30
S-29	[40]	2	2	1	0	1.30
S-30	[41]	2	1	1	1	1.25
S-31	[42]	1	1	1	2	1.25
S-32	[6]	1	1	1	2	1.25
S-33	[43]	1	1	1	2	1.25
S-34	[44]	1	2	2	0	1.25
S-35	[45]	1	2	2	0	1.25
S-36	[46]	1	2	2	0	1.25
S-37	[47]	1	2	2	0	1.25
S-38	[48]	2	1	2	0	1.20
S-39	[49]	1	1	2	1	1.20
S-40	[50]	2	1	2	0	1.20
S-41	[51]	2	1	2	0	1.20
S-42	[52]	2	1	2	0	1.20
S-43	[53]	2	2	0	0	1.10
S-44	[54]	2	2	0	0	1.10
S-45	[55]	0	2	0	2	1.10
S-46	[56]	1	1	0	2	1.05
S-47	[57]	1	2	1	0	1.05
S-48	[58]	1	2	1	0	1.05
S-49	[59]	1	2	1	0	1.05
S-50	[60]	1	2	1	0	1.05
S-51	[61]	1	2	1	0	1.05
S-52	[62]	1	2	1	0	1.05
S-53	[63]	1	2	1	0	1.05
S-54	[64]	1	2	1	0	1.05
S-55	[65]	1	2	1	0	1.05
S-56	[66]	0	1	0	2	1.05
S-57	[67]	2	1	1	0	1.00
S-58	[68]	2	1	1	0	1.00
S-59	[69]	2	1	1	0	1.00
S-60	[70]	2	1	1	0	1.00
S-61	[71]	0	1	1	2	1.00
S-62	[72]	0	1	1	2	1.00
S-63	[73]	0	2	2	0	1.00
S-64	[74]	2	1	1	0	1.00
S-65	[75]	2	1	1	0	1.00

- Cultural and policy considerations
- Industry collaboration and public-private partnerships
- Integration of skills and competencies into cybersecurity education frameworks

This mapping demonstrates that the thematic synthesis provides empirical support for each component in Fig. 5, enabling the development of a context-aware cybersecurity education framework tailored to Malaysia.

These seven categories capture the primary areas of emphasis in cybersecurity education frameworks relevant to Malaysia. The following subsections discuss each in detail, analyzing their significance and incorporation within current frameworks.

1) Cybersecurity framework development in Malaysian higher education: The reviewed studies examine the design, development, and implementation of cybersecurity education frameworks within Malaysian higher education, addressing both theoretical foundations and practical applications.

Several works emphasize pedagogical innovation and curriculum integration. For instance, [1] explores gamified learning through Capture-the-Flag competitions to enhance student engagement and technical proficiency, while [34] presents a hybrid program that combines network security and digital forensics to bridge multidisciplinary gaps. Similarly, [2] investigates the integration of penetration testing into information security curricula to strengthen practical competencies.

Other studies focus on institutional and governance perspectives. [20] proposes an information security framework tailored to Malaysian academic environments, and [6] evaluates the implementation of cybersecurity risk management frameworks across Malaysian universities.

Collectively, these studies underscore growing efforts to align cybersecurity education with both academic standards and industry practices, yet they also reveal the absence of a unified, context-specific national framework guiding higher education institutions in Malaysia.

2) International standards and local adaptation: This category examines how international cybersecurity education standards and models are adapted to align with Malaysia's regulatory, institutional, and cultural contexts. [5] evaluates the integration of global cybersecurity standards within Malaysian university frameworks, emphasizing the need for contextual alignment with national policies. [2] discusses the implementation of penetration testing practices adapted to suit local organizational requirements, highlighting the balance between international best practices and domestic applicability. Similarly, [32] raises concerns regarding the direct transplantation of international programs into local higher education systems without adequate localization.

Collectively, these studies underscore the necessity of customizing international cybersecurity education models to fit Malaysia's specific regulatory environment, institutional capacities, and cultural dimensions, ensuring both global relevance and local effectiveness.

3) Professional certifications and industry alignment: Integrating professional certifications into cybersecurity curricula is a critical step toward producing industry-ready graduates. Certifications such as CISSP, CEH, and CompTIA Security+ not only validate technical proficiency but also serve as standardized indicators of professional competence recognized globally. [28] provides guidelines for embedding these certifications into curriculum design to ensure alignment between academic outcomes and evolving industry standards. Using the Analytic Hierarchy Process (AHP), [4] models

and prioritizes essential skill sets, demonstrating how specific certifications can bridge the gap between theoretical knowledge and workplace requirements. Similarly, [3] emphasizes that aligning curriculum benchmarks with professional certification standards enhances both curriculum relevance and graduate employability.

Overall, the reviewed studies collectively highlight that embedding professional certifications within cybersecurity education supports a dynamic, outcome-oriented learning approach that keeps pace with rapid technological advancements and industry expectations—an essential consideration for developing a Malaysian cybersecurity education framework.

4) Hands-on learning and experiential education: Practical and experiential learning approaches play a vital role in developing competent cybersecurity professionals capable of addressing real-world threats. Several studies emphasize the use of hands-on techniques, such as gamification, secure coding, and virtual simulations, to bridge the gap between theoretical instruction and practical application. [1] utilizes gamified learning through Capture the Flag (CTF) competitions, which enhance student motivation and problem-solving abilities. Similarly, [44] integrates secure coding modules into non-security courses, fostering a broader understanding of cybersecurity principles across disciplines. [30] advocates for virtual laboratories and simulation environments that replicate real-world attack and defense scenarios, enabling students to apply theoretical concepts in controlled settings. Furthermore, [70] highlights the use of gamified cyber ranges to increase engagement and improve hands-on technical proficiency.

Collectively, these studies underscore that experiential learning fosters active engagement, critical thinking, and technical confidence—key competencies for preparing an industry-ready cybersecurity workforce in Malaysia.

5) Cultural and policy considerations: An effective cybersecurity education framework must account for national regulatory structures and institutional cultures to ensure both compliance and contextual relevance. In the Malaysian context, [76] examines how information security culture influences policy implementation in Klang Valley universities, highlighting the importance of fostering a shared understanding of cybersecurity values among academic stakeholders. Similarly, [43] emphasizes the need for regulatory compliance by proposing a framework that integrates information security policies into institutional governance structures.

Together, these studies illustrate that addressing cultural and policy dimensions is essential for developing sustainable cybersecurity education frameworks in Malaysia—frameworks that not only meet technical standards but also align with local values, governance practices, and regulatory expectations.

6) Industry collaboration and public-private partnerships: Collaboration between academia and industry plays a pivotal role in ensuring that cybersecurity curricula remain aligned with evolving workforce demands and technological advancements. The study [34] highlights the importance of government and industry support in the co-development of network security programs, illustrating how such partnerships enhance curriculum relevance and practical skill development. Similarly, [48] reports on the successful integration of a penetration testing module designed in collaboration with industry professionals, which significantly improved students' exposure to real-world cybersecurity challenges.

Collectively, these studies emphasize that effective cybersecurity education in Malaysia depends on sustained engagement between higher education institutions, government agencies, and the private sector. Such collaboration not only strengthens curriculum design but also supports knowledge transfer, internship opportunities, and the development of industry-ready graduates. These findings reinforce the broader categories identified in this review—technical integration, experiential learning, industry collaboration, and local adaptation—as critical components of comprehensive cybersecurity.

7) Integration of skills and competencies into cybersecurity education frameworks: Several studies have examined the identification and integration of essential skills and competencies within cybersecurity education frameworks. The study [34] discusses the development of a hybrid program in Malaysian higher education institutions that combines network security and digital forensic curricula, guided by the ISCIP common body of knowledge to ensure alignment with essential technical competencies. Building on this, [4] explores the skillsets required by the Malaysian cybersecurity job market, proposing a structured competency model based on the Analytical Hierarchy Process (AHP) that emphasizes both technical expertise and soft skills such as communication and teamwork.

At the international level, [3] highlights the significance of professional certifications in shaping cybersecurity curricula, offering a benchmark to align academic programs with recognized industry standards and competencies. Complementing this approach, [51] introduces an interdisciplinary educational framework for cybersecurity workforce development that promotes secure design thinking and integrates emerging knowledge areas through experiential learning.

Collectively, these studies underscore the importance of systematically embedding both technical and non-technical competencies into cybersecurity curricula. Such integration is crucial to ensure that graduates are not only conceptually knowledgeable but also equipped with the practical and adaptive skills required to meet the demands of Malaysia's rapidly evolving cybersecurity landscape.

IV. Findings and Results

A. Data Analysis

Fig. 3 and Fig. 4 illustrates the distribution of studies across thematic categories derived from the synthesis. A quarter of the studies (25%) focused on integrating frameworks and skills into curricula to produce an industry-ready workforce. Another 20% emphasized hands-on learning through practical activities and gamification to enhance cybersecurity education. A total of 17% highlighted the importance of industry collaboration and professional certifications—such as ISC2, CompTIA, GIAC, EC-Council, ISACA, and Offensive Security—in preparing the workforce to address current challenges in the cybersecurity landscape. Similarly, 17% of the studies discussed cultural and contextual factors specific to Malaysia. An additional 15% addressed assessment and evaluation challenges, stressing the need for effective mechanisms to prepare for future demands, while 6% of the studies focused on governance of cybersecurity education.

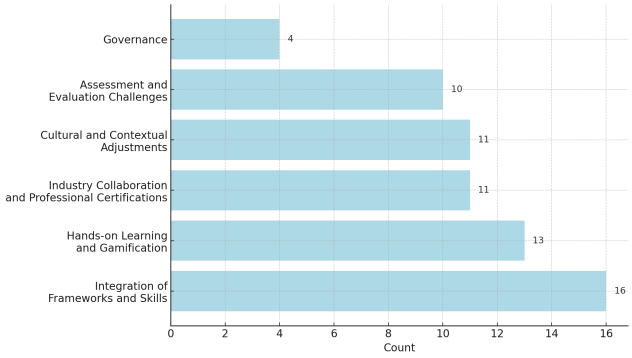

Fig. 3. Category-wise distribution of studies (bar chart).

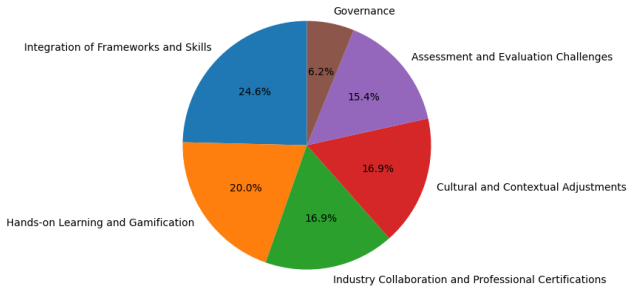

Fig. 4. Category-wise distribution of studies (pie chart).

This distribution underscores an increasing shift toward experiential and competency-based learning but also reveals comparatively limited attention to governance and evaluation mechanisms in Malaysian higher education, indicating potential areas for further development.

B. Key Findings

Building upon the categories discussed earlier in Section III-C, Table V provides a comparative overview of how the selected studies address different components of cybersecurity education in Malaysia. The findings indicate that Malaysian cybersecurity education frameworks are progressively evolving to integrate three core dimensions—technical competencies, policy awareness, and hands-on learning experiences. However, the extent and consistency of this integration vary significantly across institutions.

1) Findings related to RQ1-Current practices in cybersecurity education: The analysis revealed that Malaysian higher education institutions primarily focus on foundational technical skills and international certifications such as CISSP, CEH, and CompTIA Security+. Approximately 25% of the studies reviewed emphasized integrating these elements into the curriculum. However, hands-on learning methods—such as cyber ranges, Capture the Flag (CTF) competitions, and simulations—are inconsistently implemented across institutions. Moreover, few programs incorporate interdisciplinary components, soft skills, or ethical training, despite the industry's growing demand for holistic cybersecurity professionals. There is also a lack of formal evaluation frameworks to assess learning outcomes or curriculum impact.

These findings suggest that while the foundational structure of cybersecurity programs is strong, there is an urgent need to institutionalize experiential learning and competency-based evaluation mechanisms to ensure workforce readiness.

2) Findings related to RQ2-Challenges in curriculum–industry alignment: The review identified several barriers impeding effective alignment between academia and the cybersecurity industry in Malaysia. A key challenge is the limited collaboration between universities and industry partners, which restricts the integration of real-time, workplace-relevant skills into academic programs. Furthermore, many programs rely on global frameworks that do not adequately reflect Malaysia's regulatory requirements, cultural norms, or organizational practices. Only 17% of the reviewed studies explicitly addressed Malaysia-specific issues. The absence of structured industry advisory boards, systematic feedback mechanisms, and agile curriculum revision processes further widens the gap between academic output and industry demand.

This misalignment highlights the need for an adaptive governance mechanism that institutionalizes industry participation in curriculum design, ensuring that cybersecurity graduates meet evolving national and sectoral needs.

3) Findings related to RQ3-Framework improvements and strategic integration: The synthesis of reviewed literature suggests that an effective cybersecurity education framework for Malaysia should integrate modular, competency-based components encompassing technical expertise, policy understanding, and soft skills. Adaptation of global models such as NICE and CyBOK is essential but must be contextualized to Malaysian law, culture, and national cybersecurity strategies. Studies also emphasize the need for formalized partnerships among academia, industry, and government agencies to support curriculum co-development and experiential learning. Strategies such as gamification, internships, and cyber ranges are frequently recommended to promote real-world readiness and industry relevance.

These insights collectively point toward the development of a unified, context-sensitive framework capable of aligning Malaysia's cybersecurity education ecosystem with international best practices while preserving national relevance.

The summarized insights in Table V reinforce that while Malaysia's higher education sector has made notable progress in integrating frameworks and fostering industry partnerships, efforts remain fragmented. A national, standardized framework is therefore required to consolidate these diverse initiatives and ensure consistent competency outcomes across institutions.

C. Summary of Thematic Findings

The synthesis of the reviewed literature across the seven categories reveals a diverse but fragmented landscape of cybersecurity education in Malaysia. Collectively, the studies demonstrate significant progress in areas such as framework development, curriculum enhancement, and the integration of experiential learning. Malaysian universities have begun adopting gamified learning, virtual laboratories, and hybrid programs that merge theoretical instruction with practical exposure. Additionally, the adaptation of international standards and the inclusion of professional certifications, such as CISSP and CEH, reflect efforts to align educational outcomes with industry expectations.

TABLE V. INSIGHTS FROM KEY STUDIES ON CYBERSECURITY EDUCATION FRAMEWORKS: ANALYSIS BY CATEGORY

Category	Key Studies	Insights
Integration of Frameworks and Skills	S-1, S-4, S-15, S-17, S-19, S-27, S-29, S-34	Emphasizes integrating various cybersecurity frameworks in educational programs; aligns curricula with standards and incorporates practical skills for real-world application; recommends developing frameworks considering local industry needs, cultural factors, and Malaysian educational challenges.
Industry Collaboration and Professional Certifications	S-2, S-5, S-18, S-20, S-14, S-24	Highlights collaboration between institutions and industry stakeholders for curriculum relevance; encourages incorporating industry-recognized certifications to enhance employability; promotes partnerships that enable curriculum updates based on industry trends, keeping students current.
Cultural and Contextual Adjustments	S-3, S-10, S-12, S-8, S-23, S-31	Stresses understanding cultural and contextual factors for effective cybersecurity education; suggests adapting curricula to address regional challenges and societal expectations; recommends researching cultural impacts on learning, such as attitudes toward technology and local threat perceptions.
Hands-On Learning and Gamification	S-9, S-16, S-22, S-38, S-40, S-47	Highlights hands-on learning methods, including labs, simulations, and gamification; points to gamification's role in engagement, making learning more enjoyable and effective; advocates for immersive experiences that simulate real-world scenarios, building critical skills.
Assessment and Evaluation Challenges	S-30, S-43, S-54, S-11, S-36	Discusses the importance of effective assessment to measure program success; identifies the need for robust frameworks that accurately reflect learning outcomes; suggests innovative assessments, including project-based and real-world problem-solving tasks.
Governance	S-21, S-25, S-45, S-61, S-62	Encompasses policies, regulations, and ethical guidelines for cybersecurity education; emphasizes clear governance to support cybersecurity initiatives in higher education; calls for research into best practices, ensuring accountability and compliance with standards.

However, the review also highlights persistent challenges. Many initiatives remain institution-specific, lacking a unified national strategy or a standardised competency framework aligned with industry needs. While technical competencies are widely addressed, soft skills, management capabilities, and policy-level understanding receive comparatively less emphasis. Furthermore, few studies explicitly link educational frameworks to measurable job-readiness outcomes or industry performance indicators.

In summary, existing research underscores the importance of integrating technical, professional, and contextual competencies within cybersecurity curricula but reveals the absence of a cohesive framework tailored to Malaysia's educational and industrial ecosystem. This gap justifies the need for a structured and validated cybersecurity education framework that bridges academia and industry, ensuring that future graduates are both technically proficient and workforce-ready.

D. Proposed Cybersecurity Education Framework

Fig. 5 presents the Proposed Cybersecurity Education Framework for Malaysian Higher Education, synthesised from the literature review. The framework integrates industry requirements, competencies, and curriculum design to address the persistent gap between academia and the Malaysian cybersecurity workforce landscape.

At the upper level, the framework distinguishes between *Technical* and *Generic* (soft) skill domains. These domains shape three core components: *Knowledge and Skills*, *Tasks*, and *Competencies*. These components form the foundation of *Industry Requirements*, which is positioned at the centre of the framework. It reflects the finding that industry expectations serve as the primary driver of curriculum relevance and program design. In addition, to complement the skill domain structure of the framework, Fig. 6 provides a detailed breakdown of the technical competencies required by the Malaysian cybersecurity industry. The *Generic Competencies* encompass essential soft skills sought by the industry, including strong problem-solving ability, teamwork and collaboration skills,

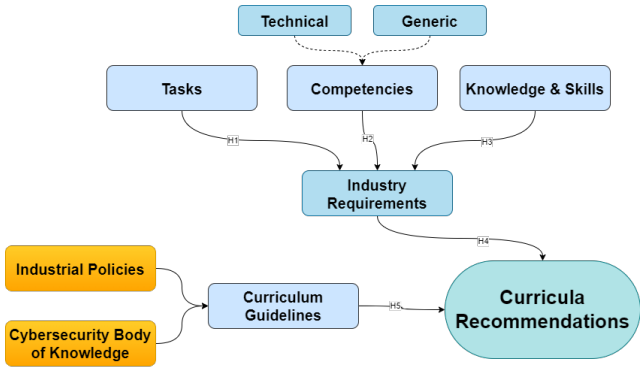

Fig. 5. Proposed Cybersecurity Education Framework synthesised from thematic findings. The framework aligns tasks, competencies, and knowledge–skills with industry requirements, guided by industrial policies and cybersecurity bodies of knowledge, resulting in actionable curriculum guidelines and recommendations for Malaysian higher education institutions.

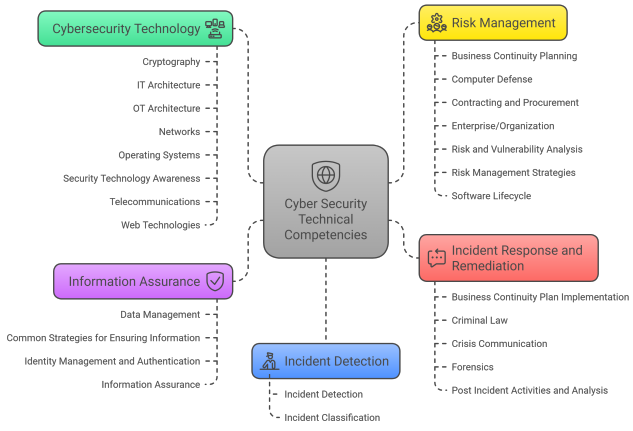

Fig. 6. List of technical competencies required by the Malaysian cybersecurity industry.

curiosity and eagerness to learn, strong communication skills, strategic thinking, project management skills, and effective time management and organization.

The framework is informed by two major external reference sources: *Industrial Policies* and *Cybersecurity Bodies of Knowledge* (e.g., CyBOK, NIST, specialised domain standards). These sources guide the formulation of *Curriculum Guidelines*, which operationalise industry requirements into implementable academic structures such as course design, learning outcomes, practical training components, and assessment strategies.

The integration of all inputs results in the generation of *Curricula Recommendations*, representing the actionable educational outputs of the framework, including curriculum revisions, certification-aligned modules, enhancement of hands-on learning components, and the establishment of industry collaborations.

How each thematic finding informs the framework:

- Cybersecurity Framework Development in Malaysian Higher Education: This theme underpins the entire structure. The progression from "Tasks–Competencies–Knowledge & Skills" toward "Curriculum Guidelines" and ultimately "Curricula Recommendations" reflects a structured cybersecurity curriculum development process tailored to Malaysian institutions.
- International standards and local adaptation: Represented in the "Cybersecurity Body of Knowledge" and "Industrial Policies" components, the framework incorporates global standards (CyBOK, NIST NICE, ISO) alongside Malaysian strategies such as MyDIGITAL and the National Cyber Security Policy.
- Professional certifications and industry alignment: Evident in the central "Industry Requirements" component and in "Curriculum Guidelines," which embed certification expectations (e.g., CISSP, CompTIA, CEH) as academic learning outcomes.
- Hands-on Learning and Experiential Education: Embedded in the "Knowledge & Skills" and "Competencies" components, driving recommendations such as cyber ranges, laboratories, CTF participation, and simulated incident response exercises.
- Cultural and Policy Considerations: Captured in the "Industrial Policies" component, ensuring alignment with Malaysian governance structures, organisational cultures, and national development priorities.
- Industry Collaboration and Public–Private Partnerships: This theme reinforces the centrality of "Industry Requirements" and supports the need for sustained partnerships through internships, expert co-teaching, industry advisory boards, and knowledge transfer programmes.
- Integration of Skills and Competencies into Cybersecurity Education Frameworks: Illustrated through the categorisation of Technical and Generic skill domains, which feed directly into competency development and curriculum design for a holistic graduate capability profile.

V. Discussion

This systematic literature review (SLR) evaluates the current state of cybersecurity education in Malaysia, revealing both significant progress and enduring challenges. While many academic programs incorporate globally recognized certifications such as CISSP and CISM, they often lack systematic alignment with Malaysia-specific regulatory frameworks, cultural contexts, and evolving industry demands. This misalignment constrains the preparedness of graduates for real-world cybersecurity challenges.

The analysis highlights that hands-on learning strategies—such as cyber ranges, Capture the Flag (CTF) competitions, and gamification—are inconsistently adopted across higher education institutions. This uneven application results in varied levels of practical competency among graduates. Standardizing experiential learning practices is therefore essential to ensure that all students develop the applied skills necessary to operate effectively in Malaysia's cybersecurity landscape. Moreover, many curricula remain static and fail to address emerging threats, new technologies, and the dynamic nature of the cybersecurity profession, thereby weakening their relevance to industry needs.

A recurring theme across the reviewed literature is the persistent disconnect between academic training and industry expectations. Industry engagement in curriculum development remains sporadic, with few structured partnerships or advisory mechanisms in place. As a result, feedback from employers and cybersecurity practitioners is not systematically integrated into educational design. The absence of robust assessment and evaluation frameworks further limits the ability to measure student proficiency and readiness for professional roles.

To address these gaps, future research and policy initiatives should focus on developing a comprehensive, Malaysia-specific cybersecurity education framework. Such a framework should harmonize global best practices—such as those derived from CyBOK and NICE—with local cultural, regulatory, and industrial contexts. It should also embed mechanisms for continuous curriculum review, stakeholder collaboration, and adaptive learning strategies responsive to technological advancements.

Furthermore, engaging industry experts through structured interviews and collaborative research initiatives can provide empirical insights into the competencies most valued in the Malaysian cybersecurity workforce. These insights can inform curriculum redesign, ensuring that future programs produce graduates equipped with both technical expertise and the adaptive, problem-solving skills required to meet Malaysia's growing cybersecurity challenges.

VI. Conclusion and Future Research Directions

This systematic literature review evaluated the current landscape of cybersecurity education in Malaysia, synthesizing insights from 65 academic and gray literature sources. The review found that while Malaysian higher education institutions have made progress in embedding technical competencies

and adopting global certifications, several critical gaps persist. These include limited experiential learning opportunities, insufficient contextual integration of local policies and cultural factors, and a lack of consistent industry-academia collaboration.

The study underscores the urgent need for a Malaysia-specific cybersecurity education framework that aligns academic curricula with industry demands while addressing national cultural and regulatory contexts. In particular, the findings highlight the importance of developing a framework that integrates hands-on pedagogical approaches, incorporates ethical and policy literacy, and reflects dynamic competency requirements as defined by both national priorities and global standards.

Future research should focus on the empirical validation of the proposed educational framework through expert interviews, surveys, or case studies. Further exploration is also needed to examine the implementation and effectiveness of experiential learning models—such as cyber ranges, gamified environments, and real-world simulations—in enhancing competency development. Continued collaboration between academic, industrial, and governmental stakeholders will be essential to sustain progressive improvements in Malaysia's cybersecurity education ecosystem.

VII. Declarations

A. Availability of Data and Material

The data used and analysed during this systematic literature review are available from the corresponding author upon reasonable request. All sources utilized in this review are publicly accessible, and references to the respective papers are provided within the manuscript.

B. Funding

This research received no external funding or financial support. The work was part of the author's ongoing academic studies.

C. Declaration of AI Assistance

The author acknowledges the use of OpenAI's ChatGPT (GPT-5) to support language refinement and structural editing in this manuscript.

References

[1] L. J. Khoo, *Design and Develop a Cybersecurity Education Framework Using Capture the Flag (CTF)*. IGI Global, 2019, pp. 123–153.

[2] C. M. Kang, P. S. Josephng, and K. Issa, "A study on integrating penetration testing into the information security framework for malaysian higher education institutions," *2015 International Symposium on Mathematical Sciences and Computing Research, iSMSC 2015 - Proceedings*, pp. 156–161, 10 2015.

[3] K. J. Knapp, C. Maurer, and M. Plachkinova, "Maintaining a cybersecurity curriculum: Professional certifications as valuable guidance," *Journal of Information Systems Education*, vol. 28, pp. 101–114, 10 2017.

[4] F. H. Sohime, R. Ramli, F. A. Rahim, and A. A. Bakar, "Exploration study of skillsets needed in cyber security field," *2020 8th International Conference on Information Technology and Multimedia, ICIMU 2020*, pp. 68–72, 10 2020.

[5] A. Aborujilah, A. Z. Al-Othmani, N. S. Hussien, S. A. Mokhtar, Z. A. Long, and M. Nizam, "Cybersecurity risk assessment approach for malaysian organizations: Malaysian universities as case study," *2022 9th International Conference on Electrical and Electronics Engineering, ICEEE 2022*, pp. 440–450, 2022.

[6] B. M. Dioubate and W. Norhayate, "Cyber security risk management frameworks implementation in malaysian higher education institutions," *International Journal of Academic Research in Business and Social Sciences*, 2022. [Online]. Available: http://dx.doi.org/10.6007/IJARBSS/v12-i4/12300

[7] R. E. McGuire, "Towards nice-by-design cybersecurity learning environments: A cyber range for soc teams," *Journal of Network and Systems Management*, vol. 32, 2024.

[8] A. Rashid, G. Danezis, H. Chivers, E. Lupu, A. Martin, and M. e. a. Lewis, "Scoping the cyber security body of knowledge," *IEEE Security & Privacy*, vol. 16, no. 3, pp. 96–102, 2018.

[9] L. Muniandy, B. Muniandy, and Z. Samsudin, "Cyber security behaviour among higher education students in malaysia," *Journal of Information Assurance & Cybersecurity*, pp. 1–13, 2017.

[10] B. M. Dioubate and W. N. Wan Daud, "A review of cybersecurity risk management framework in malaysia higher education institutions," *International Journal of Academic Research in Business and Social Sciences*, vol. 12, no. 5, pp. 1081–1093, 2022.

[11] S. R. Selamat, L. H. Hsiung, and R. Yusoff, "Development of examination framework for cyber security professional competency certification," *OIC-CERT Journal of Cyber Security*, vol. 3, no. 1, pp. 41–46, 2021.

[12] N. H. Abd Rahim, S. Hamid, and L. Mat Kiah, "Enhancement of cybersecurity awareness program on personal data protection among youngsters in malaysia: An assessment," *Malaysian Journal of Computer Science*, vol. 32, no. 3, pp. 221–245, 2019.

[13] S. M. Syed Zulkiplee, M. A. Mohd Shukran, M. R. Mohd Isa, M. A. Khairuddin, N. Wahab, and H. Hidayat, "Examining the impact factors influencing higher education institution (hei) students' security behaviours in cyberspace environment," *International Journal on Informatics Visualization*, vol. 9, no. 1, p. 2296, 2025.

[14] M. J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, and C. D. M. et al., "The prisma 2020 statement: An updated guideline for reporting systematic reviews," *International Journal of Surgery*, vol. 88, p. 105906, 4 2021.

[15] F. Samiullah, M.-L. Gan, S. Akleylek, and Y. Aun, "Group key management in internet of things: A systematic literature review," *IEEE Access*, vol. 11, pp. 77 464–77 491, 2023.

[16] B. A. Kitchenham, "Systematic review in software engineering: where we are and where we should be going," in *Proceedings of the 2nd international workshop on Evidential assessment of software technologies*, 2012, pp. 1–2.

[17] M. A. Yar, H. G. Goh, K. Adnan, M. L. Gan, and V. Ponnusamy, "Bridging cybersecurity education and industry demands: Mapping and prioritizing curriculum guidelines," in *2024 International Conference on Future Technologies for Smart Society (ICFTSS)*. IEEE, 8 2024, pp. 188–193. [Online]. Available: https://ieeexplore.ieee.org/document/10690269/

[18] D. K. K. Onayemi, "Enhancing academic cybersecurity: Integrated framework with network penetration testing," *Social Science and Humanities Journal*, vol. 7, pp. 3231–3245, 10 2023. [Online]. Available: https://www.sshjournal.com/index.php/sshj/article/view/875

[19] NACSA, "National cyber security agency (nacsa), malaysia," 2024, accessed: 21 October 2024. [Online]. Available: https://www.nacsa.gov.my/

[20] Z. Ismail, M. Masrom, Z. M. Sidek, I. Zaini, and A. M. Saaid, "Bridging information security framework for higher learning institutions of malaysia," in *International Conference on Information Management and Evaluation*. Academic Conferences International Limited, 2010, p. 483.

[21] F. Sulaiman, T. Ramayah, and A. Omar, *ICT security policy in a higher education institution in Malaysia*. IGI Global, 10 2010, vol. 1. [Online]. Available: https://www.igi-global.com/chapter/ict-security-policy-higher-education/45395www.igi-global.com/chapter/ict-security-policy-higher-education/45395

[22] C. S. Teoh, A. K. Mahmood, and S. Dzazali, "Cyber security challenges in organisations: A case study in malaysia," in *4th International Conference on Computer and Information Sciences (ICCOINS)*. IEEE, 2018, pp. 1–6. [Online]. Available: https://www.researchgate.net/publication/328604773

[23] B. Fowler, "Cybersecurity leadership policy and compliance for institutions of higher education," *https://wjaets.com/sites/default/files/WJAETS-2024-0331.pdf*, vol. 12, pp. 553–563, 10 2024. [Online]. Available: https://wjaets.com/content/cybersecurity-leadership-policy-and-compliance-institutions-higher-education

[24] S. B. M. Sabtu and K. M. Mohamad, "Critical information infrastructure protection requirement for the malaysian public sector," in *Advances in Intelligent Systems and Computing*, vol. 1188. Springer, Singapore, 2021, pp. 371–381. [Online]. Available: https://link.springer.com/chapter/10.1007/978-981-15-6048-4_32

[25] A. Parrish, J. Impagliazzo, R. K. Raj, H. Santos, M. R. Asghar, and A. J. et al., "Global perspectives on cybersecurity education for 2030: A case for a meta-discipline," in *Annual Conference on Innovation and Technology in Computer Science Education, ITiCSE*. Association for Computing Machinery, 10 2018, pp. 36–54. [Online]. Available: https://dl.acm.org/doi/10.1145/3293881.3295778

[26] I. B. Ngambeki, M. Rogers, and S. J. Bates, "Curricular improvement through course mapping: An application of the nice framework," in *ASEE Annual Conference*. American Society for Engineering Education,, 10 2021. [Online]. Available: https://peer.asee.org/36889

[27] E. Russo, M. Ribaudo, A. Orlich, G. Longo, and A. Armando, "Cyber range and cyber defense exercises: Gamification meets university students," *ACM International Conference Proceeding Series*, pp. 29–37, 12 2023. [Online]. Available: https://dl.acm.org/doi/10.1145/3617553.3617888

[28] S. Ramezanian and V. Niemi, "Cybersecurity education in universities: A comprehensive guide to curriculum development," *IEEE Access*, vol. 12, pp. 61 741–61 766, 2024.

[29] A. M. Majanoja and A. Hakkala, "Enhancing a cybersecurity curriculum development tool with a competence framework to meet industry needs for cybersecurity," in *ACM International Conference Proceeding Series*, vol. 23. Association for Computing Machinery, 6 2023, pp. 123–128. [Online]. Available: https://dl.acm.org/doi/10.1145/3606305.3606325

[30] S. Abraham and L. Shih, "Towards an integrative learning approach in cybersecurity education," in *InfoSec '15: Proceedings of the 2015 Information Security Curriculum Development Conference*. Association for Computing Machinery (ACM), 10 2015, pp. 1–1. [Online]. Available: https://dl.acm.org/doi/10.1145/2885990.2886001

[31] M. Erickson and P. Kim, "Designing cybersecurity curriculum: Exploring the need for industry certifications and experiential learning," *Issues in Information Systems*, vol. 22, pp. 9–20, 2021. [Online]. Available: https://doi.org/10.48009/4_iis_2021_9-21

[32] S. N. Mogoane and S. Kabanda, "Challenges in information and cybersecurity program offering at higher education institutions." in *ICICIS*, 2019, pp. 202–212.

[33] X. Hanyu, W. Hao, L. Qichen, Y. Qiongwei, C. Changlin, and Z. Yawen, "Exploring the gamification of cybersecurity education in higher education institutions: An analytical study," *SHS Web of Conf.*, vol. 166, p. 1036, 2023. [Online]. Available: https://doi.org/10.1051/shsconf/202316601036

[34] Z. Adnan, N. M. Amin, M. Fairuz, A. Rauf, M. Fahmi, and M. Amran, "Network security and digital forensic curricula development for private institute of higher learning (ihl) in malaysia," *Article in International Journal of Computer Applications*, vol. 180, pp. 975–8887, 2018. [Online]. Available: https://www.researchgate.net/publication/324824575

[35] P. F. Tamyez, *The Challenges and Solutions of Cybersecurity Among Malaysian Companies*. IGI Global, 2022, pp. 676–693.

[36] CyberSecurityMalaysia, "Cybersecurity malaysia," 2024, accessed: 21 October 2024. [Online]. Available: https://www.cybersecurity.my/en/index.html

[37] R. Kashef, M. Freunek, J. Schwartzentruber, R. Samavi, B. Bulgurcu, and A. K. et al., "Bridging the bubbles: Connecting academia and industry in cybersecurity research," *Proceedings - 2023 IEEE Secure Development Conference, SecDev 2023*, pp. 207–213, 2023.

[38] J. Hajny, S. Ricci, E. Piesarskas, O. Levillain, L. Galletta, and R. D. Nicola, "Framework, tools and good practices for cybersecurity curricula," *IEEE Access*, vol. 9, pp. 94 723–94 747, 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9469727/

[39] L. Williams, E. Anthi, Y. Cherdantseva, and A. Javed, "Leveraging gamification and game-based learning in cybersecurity education: Engaging and inspiring non-cyber students," *Journal of The Colloquium for Information Systems Security Education*, vol. 11, pp. 8–8, 2 2024. [Online]. Available: https://cisse.info/journal/index.php/cisse/article/view/186

[40] E. Kim and R. Beuran, "On designing a cybersecurity educational program for higher education," *ACM International Conference Proceeding Series*, pp. 195–200, 10 2018. [Online]. Available: https://dl.acm.org/doi/10.1145/3290511.3290524

[41] A. M. Almuhaideb, Saqib, and Saeed, "A process-based approach to abet accreditation: A case study of a cybersecurity and digital forensics program," *Journal of Information Systems Education*, vol. 32, pp. 119–133, 2021.

[42] B. M. Dioubate, "A review of cybersecurity risk management framework in malaysia higher education institutions," *Article in International Journal of Academic Research in Business and Social Sciences*, 2022. [Online]. Available: http://dx.doi.org/10.6007/IJARBSS/v12-i5/12924

[43] Z. Ismail, M. Masrom, Z. M. Sidek, and D. S. Hamzah, "Framework to manage information security for malaysian academic environment," *Information Assurance '—&' Cybersecurity*, vol. 2010, p. 16, 2010. [Online]. Available: http://www.ibimapublishing.com/journals/JIACS/jiacs.html

[44] L. K. Shar, C. M. Poskitt, K. J. Shim, and L. Y. L. Wong, "Xss for the masses: Integrating security in a web programming course using a security scanner," *Annual Conference on Innovation and Technology in Computer Science Education, ITiCSE*, vol. 1, pp. 463–469, 7 2022. [Online]. Available: https://dl.acm.org/doi/10.1145/3502718.3524795

[45] S. Jarocki and H. Kettani, "Examining the efficacy of commercial cyber security certifications for information security analysts," in *Proceedings - 2019 4th International Conference on Information Systems Engineering, ICISE 2019*. Institute of Electrical and Electronics Engineers Inc., 5 2019, pp. 1–5.

[46] J. D. Thompson, G. L. Herman, T. Scheponik, L. Oliva, and A. S. et al., "Student misconceptions about cybersecurity concepts: Analysis of think-aloud interviews," *Journal of Cybersecurity Education, Research and Practice*, vol. 2018, p. 5, 7 2018. [Online]. Available: https://digitalcommons.kennesaw.edu/jcerp/vol2018/iss1/5

[47] N. Kortjan and R. V. Solms, "A conceptual framework for cyber-security awareness and education in sa," *South African Computer Journal*, vol. 51, pp. 29–41, 2014.

[48] Sufatrio, J. Vykopal, and E. C. Chang, "Collaborative paradigm of teaching penetration testing using real-world university applications," in *ACM International Conference Proceeding Series*, vol. 22. Association for Computing Machinery, 2 2022, pp. 114–122. [Online]. Available: https://dl.acm.org/doi/10.1145/3511861.3511874

[49] E. Stavrou and I. Polycarpou, "Cybersecurity-related curriculum for diverse postgraduate cohorts: A case study," in *The 18th International Conference on Education and Information Systems, Technologies and Applications: EISTA 2020*, 6 2020. [Online]. Available: http://www.iiis2020.org/imsci/website/default.asp?vc=5https://www.uclan.ac.uk/research/index.php

[50] Y. Kose, M. Ozer, M. Bastug, S. Varlioglu, O. Basibuyuk, and H. P. Ponnakanti, "Developing cybersecurity workforce: Introducing cybersec labs for industry standard cybersecurity training," in *Proceedings - 2021 International Conference on Computational Science and Computational Intelligence, CSCI 2021*. Institute of Electrical and Electronics Engineers Inc., 2021, pp. 716–721.

[51] F. Sharevski, A. Trowbridge, and J. Westbrook, "Novel approach for cybersecurity workforce development: A course in secure design," in *ISEC 2018 - Proceedings of the 8th IEEE Integrated STEM Education Conference*, vol. 2018-January. Institute of Electrical and Electronics Engineers Inc., 4 2018, pp. 175–180.

[52] M. A. Rob, "It certification: Demand, characteristics and integration into traditional university mis curriculum," *Communications of the IIMA*, vol. 14, p. 2, 10 2015. [Online]. Available: https://scholarworks.lib.csusb.edu/ciima/vol14/iss1/2

[53] M. R. Asghar and A. Luxton-Reilly, "A case study of a cybersecurity programme curriculum design, resource management, and reflections," in *SIGCSE 2020 - Proceedings of the 51st ACM Technical Symposium on Computer Science Education*, 10 2020, pp. 16–22. [Online]. Available: https://dl.acm.org/doi/10.1145/3328778.3366918

[54] Q. Liu, W. Zhao, R. Wang, and J. Shi, "A competence-based three-layer cybersecurity education framework and its application," *ACM International Conference Proceeding Series*, pp. 54–60, 7 2021. [Online]. Available: https://dl.acm.org/doi/10.1145/3472634.3472649

[55] B. M. Dioubate, W. D. W. Norhayate, Z. F. Anwar, S. Fauzilah, H. M. Faiz, and L. O. Hai, "The role of cybersecurity on the performance of malaysian higher education institutions," *Jurnal Pengurusan*, vol. 67, pp. 31–41, 2023. [Online]. Available: https://doi.org/10.17576/pengurusan-2023-67-03

[56] A. F. B. M. Ajis, R. B. Ahmad, S. B. Osman, and I. B. Ishak, "Catalyst of information security in malaysia higher learning institutions," in *ISCAIE 2020 - IEEE 10th Symposium on Computer Applications and Industrial Electronics*. Institute of Electrical and Electronics Engineers Inc., 4 2020, pp. 176–179.

[57] A. K. Gwenhure and F. S. Rahayu, "Gamification of cybersecurity awareness for non-it professionals: A systematic literature review," *International Journal of Serious Games*, vol. 11, pp. 83–99, 3 2024. [Online]. Available: https://journal.seriousgamessociety.org/index.php/IJSG/article/view/719

[58] J. Nwokeji, R. Matovu, and B. Rawal, "The use of gamification to teach cybersecurity awareness in information systems," in *Proceedings of the 2020 AIS SIGED International Conference on Information Systems Education and Research*, 12 2020. [Online]. Available: https://aisel.aisnet.org/siged2020/29

[59] M. Harris and K. Patten, "Using bloom's and webb's taxonomies to integrate emerging cybersecurity topics into a computic curriculum," *Journal of Information Systems Education*, vol. 26, 1 2015. [Online]. Available: https://aisel.aisnet.org/jise/vol26/iss3/4

[60] L. A. Wahsheh and B. Mekonnen, "Practical cyber security training exercises," in *Proceedings - 6th Annual Conference on Computational Science and Computational Intelligence, CSCI 2019*. Institute of Electrical and Electronics Engineers Inc., 12 2019, pp. 48–53.

[61] A. Vaish, R. Kumar, S. Bobek, and S. Sternad, "Development of cyber security platform for experiential learning," *Journal of Cybersecurity Education, Research and Practice*, vol. 2024, p. 22, 6 2024. [Online]. Available: https://digitalcommons.kennesaw.edu/jcerp/vol2024/iss1/22

[62] B. Martini and K.-K. R. Choo, "Building the next generation of cyber security professionals," in *22nd European Conference on Information Systems (ECIS 2014)*, vol. 30. Computers and Security, 5 2014, pp. 719–731. [Online]. Available: https://papers.ssrn.com/abstract=2431592

[63] A. Robles-Gómez, L. Tobarra, R. Pastor-Vargas, R. Hernández, and J. Cano, "Emulating and evaluating virtual remote laboratories for cybersecurity," *Sensors*, vol. 20, p. 3011, 5 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/11/3011/htmhttps://www.mdpi.com/1424-8220/20/11/3011

[64] A. Aliyu, L. Maglaras, Y. He, I. Yevseyeva, E. Boiten, and A. C. et al., "A holistic cybersecurity maturity assessment framework for higher education institutions in the united kingdom," *Applied Sciences 2020, Vol. 10, Page 3660*, vol. 10, p. 3660, 10 2020. [Online]. Available: https://www.mdpi.com/2076-3417/10/10/3660/htmhttps://www.mdpi.com/2076-3417/10/10/3660

[65] T. Balon and I. Baggili, "Cybercompetitions: A survey of competitions, tools, and systems to support cybersecurity education," *Educational and Information Technologies*, 2023. [Online]. Available: https://doi.org/10.1007/s10639-022-11451-4

[66] A. Ganesin, L. Supayah, and J. Ibrahim, "An overview of cyber security in malaysia," *Arabian Journal of Business and Management Review (Kuwait Chapter)*, vol. 6, p. 12, 2016.

[67] S. Furnell and E. Stavrou, "Assessing the consistency of cyber security education," in *IEEE Global Engineering Education Conference, EDUCON*. IEEE Computer Society, 2024.

[68] I. Alsmadi and M. Zarour, "Cybersecurity programs in saudi arabia: Issues and recommendations," in *1st International Conference on Computer Applications and Information Security, ICCAIS 2018*. Institute of Electrical and Electronics Engineers Inc., 8 2018.

[69] W. Wei, A. Mann, K. Sha, and T. A. Yang, "Design and implementation of a multi-facet hierarchical cybersecurity education framework," in *IEEE International Conference on Intelligence and Security Informatics: Cybersecurity and Big Data, ISI 2016*. Institute of Electrical and Electronics Engineers Inc., 11 2016, pp. 273–278.

[70] M. Jelo and P. Helebrandt, "Gamification of cyber ranges in cybersecurity education," in *20th Anniversary of IEEE International Conference on Emerging eLearning Technologies and Applications, ICETA 2022 - Proceedings*. Institute of Electrical and Electronics Engineers Inc., 2022, pp. 280–285.

[71] A. Jamil and Z. M. Yusof, "Information security governance framework of malaysian public sector," *Asia-Pacific Journal of Information Technology and Multimedia Jurnal Teknologi Maklumat dan Multimedia Asia-Pasifik*, vol. 7, 2018. [Online]. Available: http://www.ftsm.ukm.my/apjitm

[72] R. A. Munir, S. Talib, N. Nuha, A. Molok, and R. Ahmad, "Information security governance issues in malaysian government sector," *Journal of Information Systems and Digital Technologies*, vol. 5, pp. 1–18, 11 2023. [Online]. Available: https://journals.iium.edu.my/kict/index.php/jisdt/article/view/404

[73] G. Gerontakis, P. Yannakopoulos, and I. Voyiatzis, "Evaluating cybersecurity certifications: A framework for extracting educational scenarios in cybersecurity training," in *ACM International Conference Proceeding Series*. Association for Computing Machinery, 11 2023, pp. 243–248. [Online]. Available: https://dl.acm.org/doi/10.1145/3635059.3635097

[74] M. Hudnall, "Educational and workforce cybersecurity frameworks: Comparing, contrasting, and mapping," *Computer*, vol. 52, pp. 18–28, 3 2019.

[75] H. Kähkönen and V. Niemi, "Cybersecurity education," 2013.

[76] M. Mansouri, "Evaluating information security culture in higher learning institution," Ph.D. dissertation, Universiti Teknologi Malaysia, 2012.