NUANSA INFORMATIKA
Volume 20 Nomor 1, Januari 2026

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

Important Strategies in Mitigating Cyber Threats Using SLR in the Student Environment

Herdianto Sukmana*[1], Fathoni Mahardika[2], Dani Indra Junaedi[3]
[1,2,3] University of Eleven April Sumedang, Indonesia
E-mail: *[1] * herdianto12sukmana@gmail.com,[2]fathoni@unsap.ac.id, [3]dani@unsap.ac.id

Abstract

In the ever-evolving digital era, cyber threats are increasingly diverse and demand effective mitigation strategies, especially for the educational environment and students who are easy targets for human error-based attacks. This study aims to analyze the role of cybersecurity awareness as an important strategy in mitigating cyber threats using the Systematic Literature Review (SLR) approach. A review was conducted on the literature that implements four main cybersecurity frameworks, namely NIST CSF, COBIT 5, the KAMI Index, and ISO/IEC 27001. The results of the analysis show that the technological aspect alone is not enough to guarantee security; Individual and organizational awareness—especially in the education sector, SMEs, and remote work environments—has a significant contribution to lowering the risk of cyber incidents. This study emphasizes that systematic, measurable, and framework-based awareness increase can strengthen cyber defense and support the development of a security culture among students.

Keywords— *Cybersecurity Awareness, SLR, NIST CSF, ISO/IEC 27001, COBIT 5*

Submission: December 09, 2025 Accepted: January 15, 2026 Published: January 20, 2026
DOI Article: ***https://doi.org/****10.25134/ilkom.v20i1.540*

1. INTRODUCTION

Students are currently one of the largest groups of digital users who rely heavily on information technology services for daily activities, both in the learning process, academic data storage, and social interaction. The high level of use of these technologies makes them a highly vulnerable group to various forms of cyber threats, especially when awareness and understanding of information security is still low [4], [5]. A number of studies reveal that most students do not understand basic data protection practices, such as password management, device security, as well as the identification of common cyber threats such as phishing or identity theft [6], [7], [13]. This vulnerability is increasing due to the lack of information security materials in higher education curricula, as well as the lack of applicable and simulation-based training programs, even though these approaches have been proven to increase user awareness of social-engineering attacks [8], [9], [12].

Not only in the educational environment, research in the context of MSMEs, remote workers, and formal organizations also shows that the human factor is the main weak point in the cyber defense system [1], [2], [10], [20]. The findings reinforce the view that the formation of a security culture requires continuous improvement of user awareness, especially through education that is structured and appropriate to the development of threats. In addition, several studies highlight the gap between the level of cyber awareness and cybersecurity resilience, which is heavily influenced by digital behavior, attitudes towards risk, and technology usage habits among students [13], [17].

Considering the wide and diverse scope of findings, the Systematic Literature Review (SLR) approach was chosen in this study to obtain a comprehensive picture of the role of cybersecurity awareness in threat mitigation, especially in the student environment. SLR allows researchers to systematically identify patterns, consistency of findings, and research gaps based on empirical evidence from various previous studies. In addition, this method helps map security frameworks used in global research such as NIST CSF, COBIT 5, the KAMI Index, and ISO/IEC 27001 and their relevance in the

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

context of information security education and training [14],[19]. Thus, this study is directed to synthesize the literature in depth, assess the contribution of cybersecurity awareness in reducing the risk of cyberattacks, and identify the need to develop more effective educational strategies and curricula for students.

Unlike prior systematic reviews that discuss cybersecurity awareness in broader organizational contexts, this study specifically synthesizes evidence within the student environment, where intensive digital activity and behavioral vulnerabilities are consistently reported as key risk factors [4], [5], [7], [13]. The novelty of this SLR lies in its integrated approach: (1) highlighting awareness gaps and behavioral weaknesses that are unique to students [5], [6], [16], (2) emphasizing the effectiveness of experiential and simulation-based trainingssuch as phishing simulations and gamification which has been shown to improve knowledge retention and protective behavior more effectively than conventional methods [9], [10], [12], [20], and (3) mapping the findings into multiple cybersecurity frameworks, including global standards (ISO/IEC 27001, NIST CSF, COBIT 5) and the local KAMI Index, to support structured and measurable cybersecurity awareness strategies in higher education [3], [10], [14], [15]. Therefore, this review contributes not only by summarizing existing studies, but also by providing a framework-oriented perspective that can guide universities in developing sustainable cybersecurity awareness programs for students.

2. RESEARCH METHODS

This study uses the Systematic Literature Review (SLR) approach to gain a comprehensive understanding of the trends, strategies, and effectiveness of cybersecurity awareness programs in higher education settings. The SLR method was chosen because it is able to systematically identify research patterns and gaps based on the empirical evidence available in the academic literature, as recommended by previous studies [10], [14], [16].

2.1. Formulation of Research Questions (RQ)

This research is designed to answer three main questions:

1. RQ1: What is the level of cybersecurity awareness among students?
2. RQ2: What are the factors that affect cybersecurity awareness in higher education settings?
3. RQ3: How effective are the training programs, simulation methods, and implementation of security frameworks (ISO 27001, NIST CSF, COBIT 5) in increasing student awareness?

This formulation refers to the focus of previous research that emphasized the importance of mapping awareness, behavior, and the effectiveness of security training in students [4], [5], [9], [17].

2.2. Inclusion and Exclusion Criteria

Inclusion and exclusion criteria are established to ensure that all articles analyzed in SLR have high relevance to the research objectives, have adequate academic quality, and support the process of systematic synthesis of findings. The following table summarizes the criteria used in the selection process:

Inclusion Critera	**Exclusion Criteria**
Articles related to cyber threats to students	Articles that do not address students
Focus on cybersecurity awareness or mitigation	Irrelevant to cybersecurity
Articles published within the last 5–10 years	Articles under the year range of publication
Articles in English or Indonesian	Articles in languages other than English/Indonesian
Journal, conference, or scientific review type articles	Non-scientific blogs, news, opinions, or documents

Table I: Inclusion and Exclusion Criteria

The determination of inclusion criteria aims to ensure that the analyzed studies are truly related to the main focus of the research, namely cybersecurity awareness in students and higher education. The 5-10 year restriction of publication ensures that the articles used reflect the latest conditions of cyber threat development and relevant training programs, as suggested in modern research [4], [10], [14].

Meanwhile, exclusion criteria are used to filter out articles that do not make a real contribution to the synthesis process, such as non-scientific articles or publications without empirical data. It is important that SLR results remain credible, comprehensive, and evidence-based, as is the systematic research selection procedure recommended in recent SLR studies [12], [16], [19].

p-ISSN :1858-3911 **,** ***e-ISSN : 2614-5405***
https://journal.fkom.uniku.ac.id/ilkom

2.3. Literature Search Strategy

The literature search process is carried out systematically using the SLR principle to ensure that the selected articles are truly relevant to the topic of cybersecurity awareness in the student environment. Google Scholar was chosen as the primary source because it provides a wide coverage of scientific publications and has been used consistently in similar research [11].

The use of keywords such as "cybersecurity awareness", "students", "university", "information security training", "ISO 27001", and "NIST framework" refers to the recommendations of previous studies that show that the combination of these keywords is effective in mapping research on information security awareness in higher education [6], [7].

The 5-10 year range was chosen to ensure that the literature analyzed is up-to-date, relevant to cyber threat trends and modern learning approaches. In addition, language filters (English–Indonesian) are used to ensure a diversity of perspectives and accessibility of sources [12].

The search results yield about 54 articles. The selection process is then carried out based on the relevance of the title, abstract, and compatibility with the formulation of the research question. This step follows the literature review practice as suggested in the PRISMAA approach, which advocates a gradual screening process until the most relevant articles are left out [11]. From the total, 20 articles that met the criteria were selected for further analysis [2], [6], [7].

Components	Details
Database	Google Scholar
Year Range	5-10 years
Language	English & Indonesian
Key Keywords	“cybersecurity awareness”, “students”, “university”, “education security”
Additional Keywords	“information security training”, “ISO 27001”, “NIST framework”
Search String	(“cybersecurity awareness” AND “students”) OR (“information security” AND “education”)
Number of Initial Articles	54 articles
Selection Filter	Relevance of titles, abstracts, keywords, and full-text access
Final Number of Selected Articles	20 articles

Table II : Literature Search Strategy

2.4. Selection Process (PRISMAA Model)

The article selection process follows four stages of PRISMAA: identification, screening, eligibility, and inclusion.

1) Identification

The initial stage found 54 articles from Google Scholar that were relevant to the keyword.

2) Screening

A total of 22 articles were eliminated due to irrelevant titles/abstracts or duplication.

3) Eligibility

A total of 19 articles were read in full. Six articles were excluded for not providing empirical data, not focusing on students, or not using a security framework.

4) Final Inclusion

A total of 13 main articles were selected from the evaluation results [1]–[13], then 7 additional articles were added that met the latest criteria and strengthened the scope of SLR [14]–[20], resulting in a total of 20 articles being analyzed.

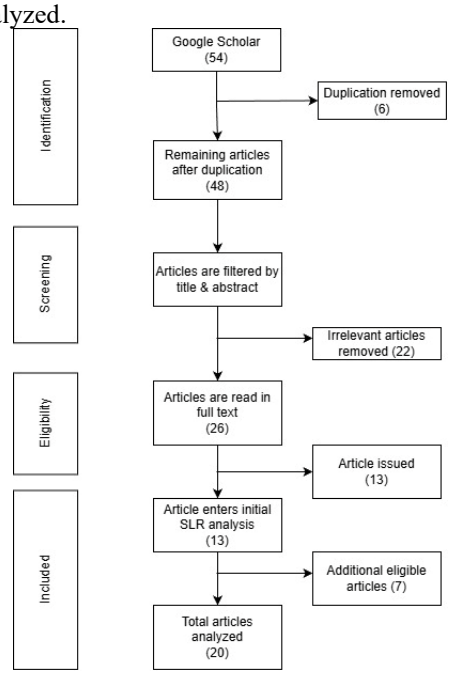


Figure 1 : PRISMA Diagram

2.5. Quality Assessment (Penilaian Mutu Studi)

To ensure the validity and credibility of the results of the Systematic Literature Review (SLR), each article selected at the final stage is further analyzed through a quality assessment

p-ISSN :1858-3911 **,** ***e-ISSN : 2614-5405***
https://journal.fkom.uniku.ac.id/ilkom

process. This quality assessment aims to ensure that the synthesised studies are of adequate methodological quality and relevant to the research focus, as recommended in SLR practice in the fields of cybersecurity and higher education [10], [14], [16].

Quality assessment was carried out by adapting evaluation criteria commonly used in SLR research, particularly those that emphasized methodological clarity and relevance of the research context [10], [16]. Each article was evaluated based on four main indicators, namely: (1) clarity of the purpose and scope of the research, (2) the suitability of the methodology with the context of cybersecurity awareness, (3) the existence of empirical data or systematic analysis, and (4) the relevance of the findings to the higher education environment or students [14], [20].

Each indicator is given a binary score (1 = meets the criteria, 0 = does not meet the criteria). Articles that obtain a minimum score of 3 out of a total of 4 indicators are declared feasible and retained in the final analysis. This approach is used to minimize bias as well as maintain the consistency and quality of the literature synthesis, as suggested in previous SLR studies [10], [16], [19].

The implementation of this quality assessment strengthens the methodological transparency of the research and ensures that the conclusions produced are truly based on credible and quality literature.

2.6. Data Extraction and Mapping of Research Questions

After the article selection process and quality assessment, a data extraction stage is carried out to identify key information from each selected study. The data extraction stage is an important component of the Systematic Literature Review (SLR) to ensure consistency, transparency, and traceability of the synthesis of findings, as recommended in previous SLR methodological studies [10], [16], [19].

The data extracted included the identity of the author and year of publication, the context and sample of the study, the method or form of cybersecurity training intervention, the security framework used, and the main findings of each study. This extraction approach refers to the common practice of SLRs in the field of cybersecurity and higher education that emphasizes the direct linkage between research findings and the formulation of research questions [14], [16].

Furthermore, each article is mapped to Research Questions (RQ1–RQ3) to identify its contribution in answering the level of cybersecurity awareness of students (RQ1), factors affecting cybersecurity awareness (RQ2), and the effectiveness of training programs and the implementation of security frameworks (RQ3). This mapping process aims to ensure that the synthesis of findings is carried out systematically and evidence-based, in accordance with the SLR approach recommended in the literature [10], [19].

Author	**Study Focus**	**Framework**	**RQ**
Fattah et al. (2023)	Student Surveys & Training	Knowledge–Attitude–Behavior	1,2
Bottyán (2023)	Student literacy survey	Model survei awareness	1
Janeš et al. (2024)	Student phishing simulation	Behavior-based training	3
Rijal et al. (2024)	Campus risk analysis	ISO/IEC 27001	2,3
Sodikin & Hikmawan (2023)	Security gamification	Gamification model	3
Goliath et al. (2024)	Attitude & behavior survey	Cyber resilience model	1,2
Taherdoost (2024)	Training model	NIST Cybersecurity Framework	3
Weapons (2025)	Conceptual studies of the campus	Cybersecurity culture framework	2

Table III. Data Extraction and Article Mapping

It should be noted that not all studies use formal security frameworks such as ISO/IEC 27001 or NIST CSF. Some studies adopted conceptual approaches or behavioral models to measure cybersecurity awareness, which remains relevant in answering the RQ of this study.

2.7. Synthesis and Analysis Techniques

The synthesis process in this study uses a thematic analysis approach to identify the main

p-ISSN :1858-3911 **,** ***e-ISSN : 2614-5405***
https://journal.fkom.uniku.ac.id/ilkom

patterns of literature related to cybersecurity awareness in the student environment. The results of the study showed four dominant themes that were interrelated. First, various training approaches such as workshops, e-learning, gamification, and phishing simulations have been proven to improve students' digital security literacy through experiential learning [8], [9], [12], [19]. Second, the effectiveness of the intervention was evaluated using a pre-post test method that assessed the improvement in knowledge, attitudes, and changes in digital habits after training [4], [5], [13]. Third, several studies emphasize the integration of security frameworks such as ISO/IEC 27001, NIST CSF, COBIT 5, and the KAMI Index as a guide in assessing awareness as well as developing information security curriculum in universities [1]–[3], [14], [20]. Fourth, the literature also reveals implementation challenges, including lack of institutional policy support, lack of faculty involvement, and weak digital security culture, which causes cyber threat mitigation programs to not run optimally in the student environment [7], [17], [18].

2.8. Limitations of Data Sources.

In this study, the literature search process was carried out using Google Scholar as the main source of academic databases. Google Scholar's selection is based on its ability to provide a wide range of scholarly publications, including national and international journals, conference proceedings, as well as open access articles relevant to cybersecurity topics in higher education settings [10], [16].

However, the use of a single database has a number of limitations. Several SLR methodological studies confirm that Google Scholar has the potential to display publication duplication, variations in article quality, and the risk of selection bias due to indexing mechanisms and search algorithms that are not fully transparent [10], [19]. In addition, certain reputable publications that are indexed exclusively on databases such as Scopus, IEEE Xplore, or ACM Digital Library are potentially not optimally identified [16].

Therefore, the results of this Systematic Literature Review (SLR) need to be understood in the context of the limited data sources used. Nevertheless, the application of inclusion-exclusion criteria, quality assessment, and a PRISMAA-based selection process is expected to minimize potential bias and maintain the validity of the synthesis of findings [10], [19].

3. RESEARCH RESULTS

The results showed that of the 54 articles analyzed in the initial stage, as many as 20 articles met all inclusion criteria and were used as the main source in the synthesis. Key findings indicate that increased cybersecurity awareness is influenced by three main aspects, namely the effectiveness of training methods, the implementation of security frameworks, and user behavior factors. Training methods such as workshops, e-learning, gamification, and attack simulations have been proven to improve basic understanding and skills in detecting and responding to cyber threats. In addition, the integration of frameworks such as ISO/IEC 27001, NIST CSF, COBIT 5, and local evaluation models helps institutions assess readiness levels and build more structured awareness standards. The study also found that behavioral factors including digital habits, policy compliance, and individual vigilance levels have a significant role in the success of cybersecurity programs. Overall, the SLR results show that increasing awareness requires a comprehensive approach that incorporates training, policies, and digital culture change in the user environment.

4. DISCUSSION

4.1. Lack of Awareness Among Students

Research findings indicate that cybersecurity awareness among university students remains relatively low. Many students still use weak passwords, rarely update them, and do not consistently apply two-factor authentication. This condition is exacerbated by limited digital literacy, the absence of institutional standard operating procedures (SOPs) for incident response, and the misconception that cybersecurity is solely the responsibility of technical staff. Several studies also report a strong relationship between formal training programs and increased awareness, which leads to safer digital behavior.

Low awareness is reflected in students' daily digital habits, including the tendency to ignore security warnings, access public Wi-Fi without protection, and share personal information through social media without considering potential risks. This suggests that students often lack contextual understanding of the consequences of cyberattacks, such as data theft, identity abuse, and account compromise. Furthermore, surveys show that only a small proportion of students are familiar with campus reporting procedures for cyber incidents,

p-ISSN :1858-3911 **,** ***e-ISSN : 2614-5405***
https://journal.fkom.uniku.ac.id/ilkom

indicating limited institutional support for awareness-building.

To address these issues, universities should strengthen preventive measures by integrating cybersecurity awareness into structured educational programs. Basic protective behaviors such as avoiding suspicious links, maintaining account confidentiality, and enabling authentication mechanisms should be promoted through continuous training and supported by clear institutional policies.

4.2. Effectiveness of Training and Simulation

Simulation-based training programs such as phishing simulation and gamification have proven to be more effective than conventional learning. This approach improves students' ability to recognize real cyber threats and significantly strengthens protective behavior. This confirms that the use of risk-based training modules and case studies encourages students to understand the real impact of information security negligence.

Some institutions have tried to implement simulation-based cybersecurity training. This approach is considered more effective than conventional learning methods. For example, training that mimics a phishing attack in a controlled environment can show first-hand how students react to real-life scenarios. In training like this, students receive fake emails that resemble real phishing attacks. Their responses were then analyzed to measure their level of alertness and ability to recognize threats.

In addition, e-learning and gamification-based training has also been proven to increase students' interest in learning. Platforms such as interactive quizzes, educational games, and real-life case-based modules make the learning process more fun and applicable. Students become more active in recognizing risks and understanding ways to avoid them. For example, in some training programs, students are asked to play the role of 'attacker' and 'victim' to better understand the point of view from both sides.

Simulation-based training is a learning method that puts students in real or near-reality situations. For example:

- Phishing simulation: students receive fake emails, then analyze their responses,
- Educational games: such as CTF (Capture The Flag) that trains tactical responses to threats,
- Real-life case module: campus digital incident analysis or data leak simulation,
- Blended learning training: combines theory and hands-on practice.

This training shows that:

- The rate of knowledge retention is higher than that of theoretical lectures,
- Students are more critical and active towards suspicious digital content,
- Participation increases if the material is interactive and challenging,
- Students feel responsible for the security of their accounts and personal devices.

Other advantages:

- Students learn from mistakes safely.
- The material is more relevant to everyday digital life,
- Can be done online and flexibly,
- Encourage the creation of a collaborative learning community.

However, this training must be carried out on an ongoing basis. One-time training without follow-up is often not enough to form a habit. Therefore, it is necessary to schedule regular sessions, periodic evaluations, and integration in the curriculum.

4.3. The Role of Frameworks in Education

Frameworks such as ISO/IEC 27001 and NIST CSF provide a systematic foundation for campuses to develop security and training policies. The implementation of this framework not only increases technical awareness but also strengthens students' managerial literacy towards information security governance.

More than that, the application of this framework in the classroom also helps lecturers in compiling teaching materials

p-ISSN :1858-3911 **,** ***e-ISSN : 2614-5405***
https://journal.fkom.uniku.ac.id/ilkom

that are structured and in accordance with industry practices. Through this approach, students not only understand theory, but are also able to map risks and design basic security policies that are relevant to the everyday digital context. Case study-based practicum activities using framework elements have also been carried out in several universities, where students are asked to audit simple security systems and make recommendations for improvement.

Frameworks such as ISO/IEC 27001 and NIST CSF help students understand information security structures systematically. Some of the implementation practices on campus include:

- Practicum makes security policies based on ISO 27001,
- Risk analysis of daily digital activities using the NIST framework,
- Group discussions on case studies of the implementation of the framework in educational institutions,
- The application of mini audits by students to the campus digital system.

This framework reinforces:

- Technical and managerial literacy of students.
- Readiness to enter the world of work based on industry standards,
- Collaboration between the IT faculty and the campus security department,
- Awareness of the importance of a proactive, not reactive, approach.

Furthermore, with the introduction of this framework since college, students can understand that information security is a comprehensive process, starting from policy making, asset identification, to access control. This knowledge is not only relevant for IT graduates, but also for students from other majors such as business, communications, and law.

4.4. Challenges of Implementation on Campus

The main challenges include limited resources for security expert lecturers, lack of cyber laboratories, and low institutional policy support. Some universities have tried to address this with programs such as "Digital Security Month" and collaborations with BSSN. However, the results of the evaluation show that without continuous training and integration into the curriculum, its effectiveness is still limited.

The implementation of cybersecurity awareness still faces challenges such as:

1. Policies not yet prioritized:
    - Awareness has not entered compulsory courses,
    - Lack of modules or guidance from institutions,
    - There is no roadmap for the development of digital competencies as a whole.
2. Resource limitations:
    - The lack of lecturers who master the field of information security,
    - Not all campuses have laboratories or security simulation tools,
    - The budget for training and platform development is still limited.
3. Permissive digital culture:
    - Students tend to be ignorant of system warnings,
    - Digital information is disseminated without thinking about the consequences,
    - There is a perception that security is the responsibility of the technician, not the user.

Nevertheless, there are good practices that can be emulated:

Regular programs such as "Digital Safety Month" and "Hoax-Free Day",

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

Collaboration with institutions such as BSSN or local security startups,

Integration of digital security materials in new student orientation,

Organizing information security education video competitions,

Creating a community of students who care about cybersecurity.

These steps are proven to be starting to build a culture of digital security awareness among students and lecturers. If it continues to be developed and supported by strong institutional policies, the campus can become a pioneer of cybersecurity awareness in Indonesia. This will make a real contribution to creating a smart, safe, and

4.5. Cybersecurity Awareness Strategy Framework in the Campus Environment

Based on the synthesis of findings in the previous section, this study not only provides an overview of the condition of student cybersecurity awareness, but also produces a conceptual strategy framework that can be applied in the campus environment. The framework is designed as a practical guide for higher education institutions in raising cybersecurity awareness in a structured and sustainable manner.

This strategic framework is built on three main pillars. The first pillar is training (*training*), which emphasizes the importance of a sustainable and experience-based cybersecurity education program. The training not only focuses on delivering theoretical material, but also involves simulated attacks, case-based learning, and interactive activities that encourage students to recognize and respond to cyber threats firsthand.

The second pillar is institutional policy (*Stuart T*). Higher education institutions need to have information security policies that are clear, easy to understand, and relevant to daily academic activities. The policy includes account management, personal data protection, incident response procedures, and the division of roles and responsibilities between students, lecturers, and system managers. Policy clarity is an important foundation for security practices to be applied consistently.

The third pillar is the formation of a cybersecurity culture (*security culture*). A culture of security is built through safe digital habits, active participation of the entire academic community, and continuous support from institutional leaders. Without a strong safety culture, the effectiveness of training and policies tends to be temporary and unsustainable.

The integration of the three pillars forms a strategic roadmap that the campus can use in designing cybersecurity awareness improvement programs. This framework allows higher education institutions to move from a reactive approach to a proactive approach in dealing with cyber threats, particularly those involving human factors in the student environment.

4.6. Novelty and Contributions of This Study

This Systematic Literature Review offers several contributions that distinguish it from previous SLRs on cybersecurity awareness. First, rather than examining cybersecurity awareness in a general context, this study focuses on the student environment as a high-risk population characterized by intensive digital activity and behavioral vulnerabilities. Second, the review synthesizes findings across four security frameworks including both global standards (ISO/IEC 27001, NIST CSF, COBIT 5) and a local assessment model (KAMI Index) to provide a comparative, structured perspective that is rarely addressed in earlier reviews. Third, beyond summarizing existing studies, this research proposes a practical strategy framework for campuses based on three integrated pillars (training, institutional policy, and security culture). This framework can be used as a roadmap to guide universities in implementing sustainable, measurable, and

p-ISSN :1858-3911 **,** ***e-ISSN : 2614-5405***
https://journal.fkom.uniku.ac.id/ilkom

evidence-based cybersecurity awareness initiatives.

5. CONCLUSION

Cybersecurity awareness is a fundamental factor in reducing vulnerability to cyber threats in the higher education environment. The results of this study show that training programs designed with interactive methods—such as phishing simulations, gamification, and scenario-based training modules—drive significant improvements in student understanding, alertness, and behavioral changes in the use of digital technology. This approach not only helps students recognize attack patterns, but also strengthens their ability to make secure decisions when interacting with information systems.

Beyond confirming the importance of cybersecurity awareness, this study offers a novel contribution by focusing specifically on students as a high-risk population and by synthesizing multiple cybersecurity frameworks—ISO/IEC 27001, NIST CSF, COBIT 5, and the KAMI Index—within a single strategic model. The proposed three-pillar framework (training, institutional policy, and security culture) provides a practical and integrative roadmap for higher education institutions, which has been largely absent in prior systematic reviews.

In addition, the integration of security frameworks such as ISO/IEC 27001 and the NIST Cybersecurity Framework into learning has been proven to provide a systematic foundation in shaping a digital security culture. The framework helps educational institutions develop more structured strategies, ranging from risk management, access control, to incident response procedures. As a result, students gain a more comprehensive understanding of the globally applicable security practice standards.

Overall, this study confirms that the combination of experience-based training methods and the application of international security frameworks is an effective step in increasing students' readiness to face increasingly complex and dynamic cyber threats. These findings also underscore the importance of educational institutions' commitment to providing ongoing training programs to build a strong information security culture in the academic environment.

6. RECOMMENDATIONS

This research is suggested to strengthen the methodological aspect of SLR by explaining the article selection process in a more structured and in-depth manner. Stages such as the number of initial findings, screening steps, elimination based on inclusion-exclusion criteria, and the final number of articles analyzed need to be described in detail so that methodological transparency can be maintained. In addition, the research also needs to add a quality assessment component to assess the methodological feasibility of each selected article, so that the conclusions produced have a stronger, valid, and accountable basis. The implementation of this quality assessment will help ensure that only relevant and academic literature of adequate academic standards is used in SLR analysis.

Further research is suggested to expand the database sources by involving reputable platforms such as Scopus, IEEE Xplore, or ACM Digital Library to obtain a more comprehensive coverage of the literature and reduce the potential for selection bias. In addition, the use of more than one database allows for stronger study replication and increases the validity of the findings in the Systematic Literature Review in the field of educational cybersecurity.

REFERENCES

[1] M. Hijji and G. Alam, “Cybersecurity Awareness and Training Framework for Remote Working Employees,” 2022.
[2] F. Ugbebor, O. Aina, M. Abass, and D. Kushanu, “Employee Cybersecurity Awareness Training Programs Customized for SME Contexts to Reduce Human-Error Related Security Incidents,” 2024.
[3] D. M. Rijal et al., “Information Security Awareness Analysis of the Threat of Data Leakage in Educational Institutions with the ISO 27001 Framework,” 2024.
[4] A. Fattah, W. Wagimin, and N. Nurlia, “Enhancing Cybersecurity Awareness among University Students: A Study on the Relationship between Knowledge, Attitude, Behavior, and Training,” JSI: Jurnal Sistem Informasi, vol. 15, no. 1, 2023.
[5] L. Bottyán, “Cybersecurity awareness among university students,” J. Applied Technical and Educational Sciences, vol. 13, no. 3, 2023.
[6] K. A. Y. Yaseen, “Importance of Cybersecurity in The Higher Education Sector,” Asian J. of Computer Science and Technology, vol. 11, no. 2, 2022.

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

[7] A. Alabab et al., "Cybersecurity Awareness of College Students in a Private Higher Education Institution," CGCI Int. J. of Administration, Management, Education and Technology, vol. 1, no. 1, 2024.
[8] A. Hakimi and M. F. Zolkipli, "An Awareness of Cybersecurity Risk Assessment and Management Among Students," Borneo Int. J., vol. 7, no. 4, 2024.
[9] R. A. Sodikin and R. Hikmawan, "Analysis of Gamification in Cybersecurity Education for Students: A Systematic Literature Review," J. Educative: Journal of Educational Studies, vol. 8, no. 2, 2023.
[10] H. Taherdoost, "Towards an Innovative Model for Cybersecurity Awareness Training," Information, vol. 15, no. 9, 2024.
[11] O. C. Okeke and C. E. Amaechi, "Awareness of Phishing Attacks in Institutions of Higher Learning: A Review of Types and Technical Approaches," Int. J. of Research and Innovation in Applied Science, vol. 9, no. 10, 2024.
[12] H. Janeš, K. Bilić, and M. Grgić, "Application of simulated phishing attacks for user training," Crisis Management Days, 2024.
[13] S. Goliath, P. Tsibolane, and D. Snyman, "Exploring the Cybersecurity-Resilience Gap: An Analysis of Student Attitudes and Behaviors in Higher Education," arXiv preprint arXiv:2411.03219, 2024.
[14] R. Armas, "Building a Cybersecurity Culture in Higher Education," *Information*, 2025.
[15] M. B. Barruga, "SYSTEMATIC REVIEW OF CYBERSECURITY FRAMEWORKS FOR HIGHER EDUCATION INSTITUTIONS: CHARACTERISTICS, COMPONENTS, AND CHALLENGES," *International Journal of Applied Mathematics*, 2025.
[16] Abdulrahman A. Arishi, Nazhatul H. Kamarudin, Khairul Azmi Abu Bakar, Zarina Binti Shukur & Mohammad Kamrul Hasan, "Cybersecurity Awareness in Schools: A Systematic Review of Practices, Challenges, and Target Audiences," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 15, no. 12, 2024.
[17] K. Sittitiamjan & P. Wuttidittachotti, "Bridging the Gap: How Knowledge, Attitudes, and Practices Shape Cybersecurity Awareness in Thai Education," *EDUPIJ*, 2025. EduPij
[18] MM Kumbhakar & Nagendra Kumar, "Cyber Security Awareness Among Higher Education Rural Students," 2025.
[19] Rahime B. Sağlam, Vincent Miller & Virginia N. Franqueira, "A Systematic Literature Review on Cyber Security Education for Children," *IEEE Transactions on Education*, 2023.
[20] C. Mouwers-Singh & T. Buzy Musikavanhu, "A Narrative Review on Enhancing Cybersecurity in Higher Education Institutions: The Role of Continuous Training and Awareness," *Expert Journal of Business and Management*, vol. 12, no. 2, 2024.