Pakistan Journal of Life and Social Sciences
www.pjlss.edu.pk

https://doi.org/10.57239/PJLSS-2024-22.2.001755

RESEARCH ARTICLE

Developing a Comprehensive Literature Review Framework for Cybersecurity Implementation in Education

Syarif Hidayatulloh[1], Aedah Binti Abd Rahman[2]

[1]Department of Information Technology, Faculty of Engineering, Adhirajasa Reswara Sanjaya University, Bandung, 40282, Indonesia

[2]Department of Information Communication Technology, Asia e University, Selangor, 47500, Malaysia

ARTICLE INFO

Received: Oct 31, 2024

Accepted: Dec 6, 2024

Keywords

Cybersecurity
Education
Security policy
Challenges
Awareness training
Technology infrastructure
Cyber threats
Collaboration
Data access policy
Digital transformation

Corresponding Author:

syarif.sfq@gmail.com

ABSTRACT

This study aims to review the implementation of cybersecurity policies and strategies in the education sector based on an analysis of 30 articles published between 2015 and 2024. The main focus of this research is to identify trends, challenges, and solutions in dealing with cyber threats faced by educational institutions. The analyzed articles cover a wide range of approaches, including empirical studies, literature reviews, case studies, and policy papers from different countries. The findings show that although many educational institutions have begun to adopt cybersecurity policies, there are still major obstacles such as limited funding, limited technical knowledge among staff, and lack of cybersecurity awareness. The solutions identified include cyber awareness training for staff and students, strengthening technology infrastructure, and implementing strict data access policies. The study also emphasizes the importance of collaboration between educational institutions, the private sector, and the government in strengthening defenses against cyber threats, as well as supporting a safe and sustainable digital transformation of education.

INTRODUCTION

The development of information and communication technology (ICT) has had a significant impact on the education sector, including increasing access to learning and interaction between stakeholders (Apriadi, 2023; Waskita, 2023). However, this progress is also accompanied by increasing cyber threats that can damage the security of students' personal data and the integrity of the learning process (Satrio et al., 2022; Arianto&Anggraini, 2019). These threats include increasingly sophisticated cyberattacks, which require educational institutions to implement effective cybersecurity measures (Faizal, 2023; Luthfah, 2023). The importance of awareness of cybersecurity among managers and users of educational technology is becoming increasingly urgent, considering the many cases of digital crime that occur (Sussolaikah, 2023; Hadiprakoso& Satria, 2022). Therefore, training and education on cybersecurity must be integrated into the educational curriculum to protect data and increase understanding of existing risks (Faliandy, 2023; Basri et al., 2021). This effort will not only strengthen the digital infrastructure of education, but also protect the privacy rights of individuals in accordance with applicable regulations (Juaningsih et al., 2021).

The implementation of cybersecurity in the education sector covers various important aspects, from policy formulation to security risk management. However, the challenges faced by educational institutions in implementing these measures are still quite large. Many educational institutions, especially at the primary and secondary levels, tend to consider cybersecurity as an additional priority that is only met reactively after an incident. This has the potential to cause significant losses, such as theft of students' personal data, hacking of academic administration systems, and attacks on hardware and software used in Faizal's learning process (2023).

The drafting of a clear and documented cybersecurity policy is essential to provide a framework that can be followed by all stakeholders in educational institutions. These policies should include risk identification, the use of cutting-edge protection technologies, and training and increased cybersecurity awareness among users, including students and staff (Luthfah, 2023). Additionally, it is important for educational institutions to conduct regular security evaluations and tests to ensure that existing systems remain safe from evolving threats (Arianto&Anggraini, 2019).

On the other hand, a proactive approach to managing cybersecurity risks can help educational institutions to be better prepared for potential attacks. This includes collaboration with cybersecurity institutions and the development of protection technologies that are tailored to the specific needs of the education sector (Islami, 2018). Thus, the cybersecurity measures implemented will not only protect students' personal data, but also maintain the integrity of the learning process and the stability of the overall digital infrastructure of education (Triyanto, 2020).

Some of the main problems faced in the implementation of cybersecurity in the education sector include low awareness and cyber literacy among users, be it students, teachers, or support staff. This can trigger various vulnerabilities that are often used by cybercriminals to launch attacks. On the other hand, the limited resources owned by educational institutions, both in terms of finance, technology, and experts, are also an obstacle to the development of an effective protection system. In addition, existing policies and regulations are often not able to anticipate the ever-evolving cyber threats, so many educational institutions only implement minimum protocols that are inadequate.

Previous research has discussed the importance of cybersecurity in educational institutions, but with limited coverage. Jones and Smith (2021), for example, in their study highlighted the readiness of higher education institutions to face cyberattacks and found that lack of training and user education was one of the main obstacles. Similarly, research by Rahmawati (2022) that examines data protection in high schools in Indonesia shows that cybersecurity is often limited to student data without involving the entire online learning process and system. The research of Liu et al. (2023) emphasizes the importance of management involvement in building holistic security policies, but the research only focuses on higher education institutions and formal academic systems. From various existing studies, it can be seen that the approach taken tends to be partial, only highlighting one or two aspects such as policy or training, without providing comprehensive and integrative solutions.

The gap in this study shows the need for a more holistic approach to the implementation of cybersecurity in the education sector, especially at the primary and secondary education levels. This research aims to develop a framework that includes various important elements in the implementation of cybersecurity, including policy strengthening, adoption of adaptive security technologies, and increasing cyber literacy and awareness among users. With a focus on the key challenges and risks facing educational institutions, the study will also analyze the factors that affect the effectiveness of implementing cybersecurity measures.

The main objective of the study is to design a comprehensive framework, which can be adopted by educational institutions to improve their readiness and resilience against cyber threats. This framework is expected to be able to create a safe and secure learning environment, providing a sense of trust for students, teachers, and other stakeholders. Furthermore, the contribution of this research is expected to strengthen policies and regulations in the education sector, as well as encourage the adoption of innovative security technologies to anticipate and counteract various cyber threats in the future. Thus, the effective implementation of cybersecurity will be the foundation for the creation of a safe, adaptive, and sustainable digital education ecosystem.

RESEARCH METHODS

In this study, we will conduct a systematic review to integrate various aspects relevant to the implementation of cybersecurity in the education sector. This approach is inspired by previous studies that use systematic review methodologies to provide a comprehensive overview of a particular topic (Araujo et al., 2020; Laengle et al., 2017; Mariz et al., 2018; Nascimento & Alencar, 2016; Pereira & Costa, 2015; Ruschel et al., 2017; Zopounidis et al., 2015). In the methodology adopted, the first step is to define the main needs and problems faced in the implementation of cybersecurity in an educational environment. After that, we will collect and filter the relevant literature based on the established procedures. The results of this study will be presented in a

structured manner, followed by an in-depth analysis to identify challenges, opportunities, and strategies that can be adopted to strengthen cybersecurity in the education sector.

The first step of this research is to determine issues relevant to the implementation of cybersecurity in educational institutions. This definition phase aims to identify the needs and problems that have been raised in the previous literature, which will then be presented and analyzed in a systematic review. In this phase, relevant issues are outlined to direct a series of Research Questions (RQs) aimed at guiding the analysis of results, determining the presence of gaps in the literature, and establishing the scope of the review. The following are the identified research questions (RQs), which are not sorted by level of importance:

Table 1. Research Questions (RQs)

RQ	Description
RQ 1	How has cybersecurity policy developed in the education sector in recent years?
RQ 2	Is there any development in the application of cybersecurity technology in the educational environment?
RQ 3	Has the educational institution implemented comprehensive and comprehensive cybersecurity measures?
RQ 4	What is the level of cyber literacy and awareness among students, teachers, and support staff in dealing with cyber threats?
RQ 5	Is there an integration between cybersecurity policies and the technology used to protect the education system?
RQ 6	Is there a prevalence of using training and education as a key approach to increasing cybersecurity awareness?
RQ 7	How is risk management applied to deal with and manage cyber threats in an educational environment?
RQ 8	Is there a significant integration between policy, technology, and training approaches to address cyber threats in the education sector?

By setting these research questions, our research aims to investigate the linkages between policy, technology, user awareness, and risk management in the implementation of cybersecurity in the education sector. The focus is on identifying existing challenges, analyzing limitations in the approach taken, as well as developing a holistic strategy to strengthen digital security in the educational environment. This is expected to provide relevant and applicable solutions to increase resilience to cyber threats in the education sector.

Article Collection and Selection

In this study, we used a database that includes a variety of relevant literature, with a focus on studies that examine the implementation of cybersecurity in the education sector. This dataset was collected using databases such as Google Scholar, IEEE Xplore, Scopus, and Web of Science, for a period of time between 2015 and 2024. Our search methodology is based on the use of carefully formulated keywords to capture various aspects of cybersecurity, particularly in the context of education. Two sets of keywords are used, as shown in Table 2 below. The first set consists of keywords related to cybersecurity and the education sector, while the second set focuses on approaches, technologies, and policies that support the implementation of cybersecurity in education.

Each keyword in the first group is combined with the keywords from the second group to generate a thorough search. Initially, a total of 1,500 articles were found. These articles are then filtered using standard procedures, which will be outlined below.

Table 2: Keywords Used

Cybersecurity Keywords	Keywords of Implementation in Education
Data protection; Cyber attack prevention; Cyber literacy; Digital security; Information security management; Risk management in education; Secure educational networks; Cyber policy development; Cyber threat resilience; Digital infrastructure security	Education policy on cybersecurity; Technology integration in education; Cybersecurity training in schools; Digital literacy in educational settings; Information management systems; Data protection for students; Security awareness programs; School network security; Cybersecurity frameworks in education;

	Incident response protocols in schools; Governance in educational cybersecurity

Screening Process

The screening process begins by removing articles from conferences and presentations (the "proceedings papers" category). This filter is applied to focus attention on papers that have primary academic relevance, which are categorized as "articles" and "reviews" in the research platform used. Therefore, books, presentations, and other types of publications are excluded from this review. Some articles derived from presentations at congresses that were later published in scientific journals were still included in the analysis. A total of 87 papers successfully passed Filter **1.**

Next, we apply a second filter. Since we use an extensive set of keywords to ensure comprehensive coverage, many articles can be easily excluded. For example, the keyword "Cyber literacy" resulted in several articles that are irrelevant to the educational context, such as papers that discuss digital literacy in the business sector. In addition, there are a number of papers that discuss cybersecurity in general but do not cover its application in the education sector. Articles that do not fit the purpose of the research, such as papers that only discuss theory without implementation in the world of education, are ignored in this screening. After this screening process, as many as 30 papers were selected for more in-depth analysis according to the purpose of this research.

RESULTS AND DISCUSSION

Reviewed Article Profiles

This study reviews a number of articles relevant to the implementation of cybersecurity in the education sector in the period from 2015 to 2024. A total of 30 articles that passed the selection and screening process were analyzed in depth to gain comprehensive insights into key trends and issues in cybersecurity in educational institutions. The profile of the reviewed articles includes empirical studies, literature reviews, case studies, and policy papers from different countries, reflecting a global approach to the issue.

It	Article Title	Writer	Year	Sources/Publications
1	An Offline Capture the Flag-Style Virtual Machine and an Assessment of Its Value for Cybersecurity Education	Tom Chothia, Chris Novakovic	2015	USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15)Integrating Security in the Computer Science Curriculum
5	rity Challenges on Academic Institutions and Need for Security Framework	W.M. Dar	2015	i-Manag. J. Inf. Technol.
6	(1393-JR419)r Social Engineering Awareness Program for Schools	Saba Mohammed, Edward Apeh	2016	IEEE SKIMA
7	Embeddingity in the Second Programming Course (CS2)	Michael Verdicchio, Deepti Joshi, Shankar M. Banik	2016	Journal of Computing Sciences in Colleges
8	Trends 20(06758852)g and Teaching in European Universities	Andrée Sursock	2015	European University Association
9	Maintaining a Cyberrriculum: Professional Certifications as Valuable Guidance	Kenneth J Knapp, Christopher Maurer, Miloslava Plachkinova	2017	Journal of Information Systems Education
10	Multidisciplinary Minor in Foa Small Liberal Arts University	Aparna Mahadev, Anne Falke, Penny Martin, Maura Pavao	2016	ACM Conference
11	Spears Against Shields: Are D(06758852)nning the Phishing War?	Ayman El Aassal, Rakesh Verma	2019	ACM International Workshop on Security and Privacy Analytics
12	Novel Approach for Cybersecur(1393-JR419)ce Development: A Course in Secure Design	Filipo Sharevski, Adam Trowbridge, Jessica Westbrook	2018	IEEE Integrated STEM Education Conference

13	Enhancing Cybersecurity Skill(06758852)ng Serious Games	Valdemar Švábenský, Jan Vykopal, Milan Cermak, Martin Laštovička	2018	ACM Conference on Innovation and Technology in Computer Science Education
14	This is Not a Game: Early Observations lternate Reality Games for Teaching Security Concepts	Tanya Flushman, Mark Gondree, Zachary NJ Peterson	2015	Workshop on Cyber Security Experimentation and Test
15	Cybersecurity Curricular Guidelines	Matt Bisho	2017	Springer International Publishing
16	Securing the Human: A Review of Literature on Broadening Diversity in Cybersecurity Education	Xenia Mountrouidou et al.	2019	ITiCSE Working Group Reports, ACM(3344429.3372507)
17	Phishing in an Academic Community: A Study of User Susceptibility an	Diaz, A., Sherman, A.T., Joshi, A.	2020	Cryptologia
18	Game-Based Cybersecurity Training for High School Students	Jin, G., Tu, M., Kim, T. H., Heffron, J., & White, J.	2018	ACM SIGCSE
19	Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factor	Wm. Arthur Conklin, Raymond E. Cline Jr., Tiffany Roosa	2018	Hawaii International Conference on System Sciences (HICSS)
20	Security scenario generator {{{{{SecGen}}}}}: A framework for generating randomly vulnerable rich-scenario {VMs} for learning computer security and hosting {CTF} events	Schreuders, Z. C., Shaw, T., Shan-A-Khuda, M., Ravichandran, G., Keighley, J., & Ordean, M.	2017	USENIX Workshop on Advances in Security Education
21	Human Risk Factors in Cybersecurity	Cuchta, T., et al.	2019	SIG Conference on Information Education
22	A Systematic Review of Cybersecurity Risks in Higher Education	Joachim Bjørge Ulven, Gaute Wangen	2021	Future Internet, MDPI
23	A Cybersecurity Education Programme for Students and Teachers	GenCyber Initiative	2017	NS(1393-JR419)rted Program
24	A Cross-Cultural Comparison of Online Behavioral Advertising Knowledge	V. Ratten	2015	Journal of Schnology Policy Management
25	Spam Emails in Academia: Issues and Costs	J. Teixeira da Silva, A. Alkhatib, P. Tsigaris	2020	Scien(futureinternet-13-00039...)
26	An Empirical Study of Root-Cause Analysis in Information Security Management	Wangen, G. et al.	2017	(1393-JR419)Conference
27	Data Security Obstacles and Strategies from Carolina Universities	Compton, Y.R.	2020	Walden Univers (1393-JR419) hesis
28	Challenges of Implementing Cybersecurity Education in Schools	Rahman N. A. A., Sairi I. H., Zizi N. A. (1393-JR419)F.	2020	International Journal of Information and Education Technology
29	Teaching Computer Science with Cybersecurity Education Built-In	Yue, C.	2016	USENIX ASE
30	Framework fecurity Strategy for Developing Countries	K. Salamzada, Z. Zarina, M.A. Bakar	2015	Asia-Pacific Jnformation Technology and Multimedia

Analysis of Cybersecurity Trends in Education

In the last decade, the increasing attention to cybersecurity in the educational environment cannot be ignored. This is not only triggered by the digital revolution in the education sector, but also by the increasing number and complexity of cyberattacks targeting educational institutions. Universities, schools, and other educational institutions now manage vast amounts of personal data, sensitive research, and operational information that make them easy targets for cybercriminals, including individual hackers as well as organized groups with economic or political motives. A study from Ulven and Wangen (2021) underscores that threats such as data theft, ransomware, and attacks on cloud networks are rapidly growing threats in the educational environment. These challenges are exacerbated by academic policies that encourage openness and collaboration that often run counter to strict security principles.

In response to this increasing threat, educational institutions have embarked on proactive measures to strengthen cybersecurity policies and build more advanced defense infrastructure. An article written by Conklin et al. (2014) shows how the U.S. government and educational institutions are developing frameworks such as the National Initiative for Cybersecurity Education (NICE) to address the skills gap in this area. The initiative is designed to develop a workforce that is better prepared for threats, with a focus on education that embraces the development of technical skills, ethical understanding, and a cross-disciplinary approach. The challenges in developing an effective educational program are also influenced by the difference in needs between educational institutions and the industrial world. Many academic programs still need to adapt quickly to changing technology and dynamic threat patterns, which makes them sometimes lag behind the actual needs in the field.

However, this challenge is not only about technology and regulation. A study conducted by Rahman et al. (2020) highlights the importance of cybersecurity education at the primary to secondary school levels. Children are currently exposed to digital technology from an early age, both through online learning, social media, and personal devices. Without sufficient digital awareness and literacy, they are vulnerable to becoming victims of cyberbullying, online exploitation, and other threats. Therefore, the integration of cybersecurity education in school curricula can play an important role in building security awareness from an early age and creating a generation that is more savvy and prepared to face cyber challenges.

The adoption of cloud-based platforms for online learning during the COVID-19 pandemic has also expanded the scope of cyber threats. Many schools and universities rely on cloud solutions to provide flexible and sustainable education, but this also opens up loopholes for attacks, such as data exploitation or unauthorized access breaches. In their research, Mountrouidou et al. (2019) highlighted that cybersecurity workforce diversification and culture-based skills development are essential to ensure an inclusive approach to security. This diversification includes encouraging the participation of underrepresented groups in cybersecurity, such as women and minorities.

Beyond the technical approach, other studies have also shown that strengthening cybersecurity policies requires cross-sector and inter-country cooperation. Educational institutions need to continue to innovate in developing risk mitigation strategies that focus not only on hardware or software, but also on user behavior. For example, cybersecurity awareness campaigns for students, staff, and faculty can help reduce social engineering-based attacks, which often exploit human weaknesses rather than the technology system itself. Research by various parties shows that integrating education, practical training, as well as strong security policies can create an educational environment that is more resilient to cyber threats.

In conclusion, the increasing attention to cybersecurity in the educational environment reflects the importance of maintaining the integrity of the digital learning process and protecting the data managed by educational institutions. Despite the major challenges, progressive measures, such as better integration of security policies, increased awareness, and the development of more resilient infrastructure, can help educational institutions deal with future cyber threats. Cooperation between policy makers, industry, and the education community is needed to create an ecosystem that is safe, sustainable, and in accordance with the dynamics of digital technology that continues to develop.

Cybersecurity Policies and Regulations in the Education Sector

The implementation of cybersecurity policies in educational institutions plays a very crucial role in shaping effective cyber risk protection and management. Various studies show that the success of

the implementation of cybersecurity policies is highly dependent on several factors, including the existence of national and international regulations governing cybersecurity governance, as well as adequate training for human resources (HR) involved in the management and implementation of these policies. According to research by Wangen, G. et al. (2017) in *An Empirical Study of Root-Cause Analysis in Information Security Management*, the importance of having a policy that is constantly updated is indispensable to deal with the ever-evolving threats in cyberspace. In addition, institutions that are successful in reducing the risk of cyber threats are those that consistently update policies and strengthen understanding of cybersecurity at every level of the organization, including in curriculum and training.

However, many educational institutions still face serious challenges in the implementation of this policy. One of the main challenges faced is limited funding, which hampers their ability to implement comprehensive security policies. As revealed by Compton, Y.R. (2020) in *Data Security Obstacles and Strategies from Carolina Universities*, many universities struggle to allocate sufficient funds for technological updates and ever-evolving HR training, which contributes to the low effectiveness of their cybersecurity policies. In addition, many institutions also face limitations in terms of the availability of trained experts, as well as low awareness of the importance of cybersecurity policies among staff and students, as discussed in a study by Cuchta, T., et al. (2019) in *Human Risk Factors in Cybersecurity*. Lack of awareness and training is a significant inhibiting factor in building a strong cybersecurity culture.

To address this issue, many institutions are beginning to adopt a more holistic approach in the implementation of cybersecurity policies, which involves game-based training or serious games to increase learner engagement, as described in the research by Jin, G. et al. (2018) in *Game-Based Cybersecurity Training for High School Students*. This approach has proven effective in raising awareness of the importance of cybersecurity and reducing the knowledge gap among end-users in educational environments.

Overall, the successful implementation of cybersecurity policies in educational institutions not only requires regular policy updates, but also requires the active involvement of all elements of the organization in an effort to reduce cyber risks. With strong policy support, adequate training, and continuous evaluation, educational institutions can mitigate potential cyber risks that threaten their operational sustainability and reputation.

Cybersecurity Technologies and Practices

The studies analyzed show that technology plays a key role in strengthening cybersecurity in educational settings, with a wide range of technologies being used to address cyber risks. Some of the technologies most frequently mentioned in the literature include firewalls, data encryption, intrusion detection systems (IDS), and multi-factor authentication. These technologies serve as layers of protection to prevent unauthorized access, protect sensitive data, and detect suspicious activity within the network. For example, according to research by Jin, G. et al. (2018) in *Game-Based Cybersecurity Training for High School Students*, the application of security technologies such as firewalls and IDS on an educational scale is essential to maintain the integrity of school IT systems, especially when students' personal data and academic information must be properly protected.

However, these technologies are only effective if they are implemented appropriately and within the framework of a solid security policy. One of the best practices that many recommend is the implementation of regular software updates. This serves to close security gaps that can be exploited by hackers, as well as keep the system up-to-date with the latest threats. Wangen, G. et al. (2017) in *An Empirical Study of Root-Cause Analysis in Information Security Management* suggests that educational institutions should have strict policies regarding software and other security system updates to mitigate threats that may arise from their vulnerabilities. In this case, intrusion detection systems (IDS) and multi-factor authentication can help detect penetration attempts and reduce the potential for unauthorized access, which is often a major vector in cyberattacks.

In addition, periodic training for staff and students is also an integral part of an effective safety policy. This training aims to raise awareness about good cybersecurity practices, such as recognizing phishing, managing passwords securely, and avoiding behaviors that can compromise network security. As suggested inthe *Security Scenario Generator (SecGen)* by Schreuders, Z. C. et al. (2017),

scenario-based training that simulates real-world threats can be very beneficial for training staff and student readiness in the face of potential cyberattacks. The skills gained through this simulation allow them to respond to threats more quickly and effectively.

However, while these technologies and best practices have proven effective in many institutions, there are significant gaps in implementation, especially in small schools or educational institutions that have limited resources. The main obstacles faced are budget constraints and a lack of experts trained in the field of cybersecurity. Rahman, N. A. A., et al. (2020) in *Challenges of Implementing Cybersecurity Education in Schools* emphasizes that smaller schools often struggle to allocate sufficient funds for advanced technology investments or to provide sufficient training for staff and students. In addition, awareness issues are also still a major challenge, where many staff and students do not fully understand the risks associated with cyberattacks, and how to protect their personal data as well as educational institutions.

This low awareness of the importance of cybersecurity policies and technologies often leads to suboptimal implementation, even when the policies implemented are in line with industry standards. Therefore, to address these challenges, it is important for governments and educational organizations to provide adequate financial support and training to disadvantaged schools, as well as introduce strict network access policies that can mitigate potential external threats.

Overall, although many educational institutions have implemented advanced security technologies and best practices in cyber risk management, challenges in terms of limited resources remain a major obstacle. With a more inclusive approach and supportive policies, it is hoped that this gap can be overcome, and the educational environment can be better prepared to face growing cyber threats.

Challenges of Cybersecurity Implementation in Educational Institutions

The main challenges in the implementation of cybersecurity in the education sector are complex, with various barriers that hinder the effectiveness of protection against cyber threats. One of the biggest challenges is the lack of funding, which has left many educational institutions, especially in small schools and colleges with limited resources, unable to allocate adequate budgets to purchase the latest security technologies or to carry out sufficient training. According to research by Wangen, G. et al. (2017) in *An Empirical Study of Root-Cause Analysis in Information Security Management*, many universities have difficulty funding effective security policies and systems, thus making them more vulnerable to potential cyberattacks.

In addition to funding issues,the limited technical knowledge among staff is also a major obstacle. Cybersecurity requires a deep understanding of the various threats and technologies used to deal with them, such as firewalls, intrusion detection systems (IDS), data encryption, and multi-factor authentication. Many educational institutions still lack experts trained in this field. For example, inthe *Cybersecurity Curricular Guidelines* by Matt Bisho (2017), it is explained that to be able to deal with cyber threats effectively, academic and administrative staff need to be provided with appropriate training, so that they can quickly identify potential risks and respond appropriately. Without sufficient knowledge about cybersecurity, educational institutions are vulnerable to cyberattacks, such as hacking students' personal data or ransomware attacks that can damage their operations.

Reliance on vulnerable technologies is also one of the main challenges. While educational institutions have implemented a variety of technologies to strengthen their security, many of them may not always be up-to-date or vulnerable to evolving threats. For example, firewalls and intrusion detection systems used by many institutions may be outdated and less effective in the face of more sophisticated cyberattacks. Research by Schreuders, Z. C. et al. (2017) in *Security Scenario Generator (SecGen)* states that while such technologies can help in protecting systems, they should always be updated and tested to ensure that they can cope with evolving threats. Limitations in software updates and vulnerable technological systems are the main reason why many educational institutions still experience security breaches.

Additionally, many educational institutions do not yet have adequate policies and procedures in place to handle cybersecurity incidents. In many cases, institutions do not have a clear incident response plan or structured procedures for handling and responding to cyber threats. This is very dangerous because without adequate policies, it is more difficult for educational institutions to reduce the impact of cybersecurity incidents and can even worsen the damage caused. For example, in a study

by Compton, Y.R. (2020) in *Data Security Obstacles and Strategies from Carolina Universities*, it was stated that many universities do not have a complete security policy, which can lead to an inability to handle incidents and exacerbate their vulnerability to attacks.

Resistance to change is also a factor that worsens the implementation of cybersecurity policies. Many educational staff, including lecturers, administrative staff, and students, may be reluctant to adopt new technologies or follow stricter security procedures. This often happens due to a lack of awareness of the importance of cybersecurity or the inconvenience of changing the way of working that is already familiar. As explained in a study by Rahman, N. A. A. et al. (2020) in *Challenges of Implementing Cybersecurity Education in Schools*, many educational institutions are experiencing resistance to change in terms of the adoption of new security technologies, especially among staff who lack a understanding of cyber threats and the importance of implementing stricter policies.

The lack of awareness at the user level is also very significant in hindering the effective implementation of cybersecurity. Many students, staff, and even institutional leaders are not fully aware of the potential cyber risks they face. They may not realize the importance of using strong passwords, recognizing phishing attacks, or keeping their personal data safe. Therefore, education and training on cyber threats need to be an integral part of the culture of educational institutions, as expressed by Jin, G. et al. (2018) in *Game-Based Cybersecurity Training for High School Students*, who suggested that game-based training and threat simulation can increase awareness and understanding of cybersecurity among students and staff.

Finally,the limited collaboration between educational institutions, industry, and the government is also an obstacle in increasing resilience to cyber threats. Many educational institutions do not have strong collaboration networks with the tech industry or government agencies that can provide the resources and expertise to address cyber threats more effectively. Research by Xenia Mountrouidou et al. (2019) in *Securing the Human: A Review of Literature on Broadening Diversity in Cybersecurity Education* shows that collaboration with external parties is essential in creating stronger security policies and in providing the necessary training and resources to address cyber threats.

Overall, the challenges in implementing cybersecurity policies in the education sector are greatly influenced by various factors, ranging from limited funding, limited technical knowledge, reliance on vulnerable technologies, to lack of awareness at the user level and resistance to change. To address these challenges, a more holistic approach is needed, with a focus on increased funding, ongoing training, regular technology updates, and closer collaboration between educational institutions, governments, and the industry sector.

Solutions Strategies and Approaches in Overcoming Cyber Threats

Various strategies to address cyber threats in the education sector have been widely discussed in the literature, with the aim of improving institutional resilience to increasingly complex attacks. Here are some of the key strategies proposed to address cyber threats in the education sector, along with a lengthy discussion of each:

Cybersecurity Awareness Training

Cybersecurity awareness training is one of the first steps that must be taken by educational institutions to reduce the risk of cyber threats. This training aims to improve the understanding of staff, teachers, and students about common cyber threats, such as phishing, malware, and social engineering-based attacks. Research by Jin, G., Tu, M., Kim, T. H., Heffron, J., & White, J. (2018) in *Game-Based Cybersecurity Training for High School Students* shows that game-based or simulation-based training approaches are very effective in increasing students' awareness and understanding of potential cyber threats. This kind of training not only equips individuals with basic skills in recognizing threats, but also encourages them to act proactively in keeping data and personal information safe. Training that is carried out regularly and based on real-life scenarios can increase preparedness against evolving threats.

Strengthening Technology Security Infrastructure

The application of stronger and more sophisticated technology is another important strategy in strengthening defenses against cyber threats. The use of firewalls, encryption systems, and the implementation of intrusion detection and prevention systems (IDS/IPS) are basic measures that can

be implemented to protect the network and data of educational institutions. Schreuders, Z. C., Shaw, T., Shan-A-Khuda, M., Ravichandran, G., Keighley, J., & Ordean, M. (2017) in *Security Scenario Generator (SecGen)* states that the implementation of a security system that can automatically generate threat scenarios for security system trials is very important in improving the preparedness of educational institutions to face cyber threats. With technology constantly evolving, educational institutions need to regularly update their software and systems to maintain the effectiveness of their protection against increasingly sophisticated threats. The use of the latest technology will help increase resistance to attacks as well as reduce their vulnerability.

Strict Data Access Policy

One of the important aspects of cybersecurity risk management is the strict management of data access. Regulating who can access critical data and resources in educational institutions is key to preventing information leaks and attacks from within. Wangen, G. et al. (2017) in *An Empirical Study of Root-Cause Analysis in Information Security Management* revealed that many universities fail to implement adequate data access policies, which ultimately leads to their vulnerability to cyberattacks. Strict access management includes the use of role-based access control (RBAC) and multi-factor authentication (MFA), which can restrict access to only authorized individuals and strengthen the protection of sensitive data. This policy should also include clear procedures regarding the management and recovery of data in the event of a breach or attack.

Cooperation with External Parties

The importance of collaboration between educational institutions and external parties, such as the government, the private sector, and cybersecurity experts, has been recognized by many studies. This partnership allows educational institutions to gain access to resources and expertise that they may not have internally. Matt Bisho (2017) in *the Cybersecurity Curricular Guidelines* explains that educational institutions need to collaborate with government agencies and the private sector to update security policies and protocols continuously. Governments and the private sector can provide training, resources, and the latest technology that can be used to improve protection against cyber threats. This collaboration can also open up opportunities to share information about the latest threat trends and tactics used by cybercriminals. In addition, cooperation with external parties can also help in better planning and simulation of incident response, so that educational institutions are better prepared to deal with possible attacks.

Cybersecurity Implications for Education

Cybersecurity plays a crucial role in maintaining the smooth operation of education, the quality of learning, and public trust in educational institutions. In the ever-evolving digital era, almost every aspect of educational activities—from student data management to online learning interactions—depends on information technology. Therefore, cyber threats can have a very detrimental impact if not managed properly. Destructive cyberattacks can significantly disrupt the learning process, for example by damaging the technological infrastructure that supports online learning or learning management systems. In addition, the attack can also steal students' personal data, which if it falls into the wrong hands can be misused for detrimental purposes. This can affect not only the trust of students and parents, but also damage the reputation of the educational institution which can last for a long period of time.

Research by Cuchta, T., et al. (2019) in *Human Risk Factors in Cybersecurity* shows that the biggest challenge in managing cybersecurity in educational institutions is overcoming potential human risks, such as ignorance or negligence in maintaining data security. A lack of understanding of cyber threats can lead to staff and students being targeted by phishing attacks, malware, or even deliberate data leaks.

However, research also shows that effective cybersecurity improvements can create a safer educational environment and support the sustainable digital transformation of education. Bjorge Ulven, J. and Wangen, G. (2021) in *A Systematic Review of Cybersecurity Risks in Higher Education* suggests that educational institutions should not only focus on data and system protection, but also integrate cybersecurity policies in curriculum and education management. With proactive measures, such as cybersecurity awareness training for staff and students, strengthening secure technology infrastructure, and collaborating with external parties, educational institutions can increase

resilience to cyber threats. This in turn can support the sustainability and efficiency of digital transformation in education, where technology can be used safely to support the quality of learning and educational innovation.

Better cybersecurity can also increase public trust in educational institutions. When people feel that their personal data is safe and that the learning process can run without interruption, then trust in educational institutions will increase, opening up more opportunities for further cooperation and development in the world of education.

CONCLUSION

The conclusion of this study shows that the implementation of cybersecurity policies in educational institutions is a crucial factor in protecting data and information systems that support the learning process. Although major challenges such as lack of funding, limited technical knowledge, and limited trained human resources are still faced by many educational institutions, the implementation of the right policies can significantly reduce the risk of cyber threats. Various strategies, such as cybersecurity awareness training for staff and students, strengthening technological infrastructure, and strict data access policies, have proven effective in improving resilience to cyber threats.

In addition, collaboration between educational institutions, government, and the private sector plays a crucial role in updating and strengthening cybersecurity policies. With this joint effort, educational institutions can create a safer environment, support the continuous digital transformation of education, and increase public trust in the security of the data and information they manage.

The implementation of effective cybersecurity policies not only prevents cyber threats, but also contributes to the smooth operation of education, the quality of learning, and the sustainability of innovation in the world of education. Thus, success in managing cybersecurity in the education sector will have a direct impact on improving the overall quality of education, making the world of education better prepared to face increasingly complex digital challenges.

BIBLIOGRAPHY

Chothia, T., & Novakovic, C. (2015). An Offline Capture the Flag-Style Virtual Machine and an Assessment of Its Value for Cybersecurity Education. USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15) Integrating Security in the Computer Science Curriculum.

Dar, W. M. (2015). Security Challenges on Academic Institutions and Need for Security Framework. i-Manag. J. Inf. Technol.

Mohammed, S., &Apeh, E. (2016). A Social Engineering Awareness Program for Schools. IEEE SKIMA.

Verdicchio, M., Joshi, D., & Banik, S. M. (2016). Embedding Cybersecurity in the Second Programming Course (CS2). Journal of Computing Sciences in Colleges.

Sursock, A. (2015). Trends and Teaching in European Universities. European University Association.

Knapp, K. J., Maurer, C., &Plachkinova, M. (2017). Maintaining a Cybercurriculum: Professional Certifications as Valuable Guidance. Journal of Information Systems Education.

Mahadev, A., Falke, A., Martin, P., & Pavao, M. (2016). Multidisciplinary Minor in a Small Liberal Arts University. ACM Conference.

El Aassal, A., & Verma, R. (2019). Spears Against Shields: Are We Winning the Phishing War? ACM International Workshop on Security and Privacy Analytics.

Sharevski, F., Trowbridge, A., & Westbrook, J. (2018). Novel Approach for Cybersecurity Development: A Course in Secure Design. IEEE Integrated STEM Education Conference.

Švábenský, V., Vykopal, J., Cermak, M., &Laštovička, M. (2018). Enhancing Cybersecurity Skill Building through Serious Games. ACM Conference on Innovation and Technology in Computer Science Education.

Flushman, T., Gondree, M., & Peterson, Z. N. J. (2015). This is Not a Game: Early Observations of Alternate Reality Games for Teaching Security Concepts. Workshop on Cyber Security Experimentation and Test.

Bisho, M. (2017). Cybersecurity Curricular Guidelines. Springer International Publishing.

Mountrouidou, X., et al. (2019). Securing the Human: A Review of Literature on Broadening Diversity in Cybersecurity Education. ITiCSE Working Group Reports, ACM.

Diaz, A., Sherman, A. T., & Joshi, A. (2020). Phishing in an Academic Community: A Study of User Susceptibility. Cryptologia.

Jin, G., Tu, M., Kim, T. H., Heffron, J., & White, J. (2018). Game-Based Cybersecurity Training for High School Students. ACM SIGCSE.

Conklin, W. A., Cline Jr., R. E., & Roosa, T. (2018). Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factor. Hawaii International Conference on System Sciences (HICSS).

Schreuders, Z. C., Shaw, T., Shan-A-Khuda, M., Ravichandran, G., Keighley, J., & Ordean, M. (2017). Security Scenario Generator (SecGen): A Framework for Generating Randomly Vulnerable Rich-Scenario VMs for Learning Computer Security and Hosting CTF Events. USENIX Workshop on Advances in Security Education.

Cuchta, T., et al. (2019). Human Risk Factors in Cybersecurity. SIG Conference on Information Education.

Ulven, J. B., & Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. Future Internet, MDPI.

GenCyber Initiative. (2017). A Cybersecurity Education Programme for Students and Teachers. NSERTED Program.

Ratten, V. (2015). A Cross-Cultural Comparison of Online Behavioral Advertising Knowledge. Journal of Technology Policy Management.

Teixeira da Silva, J., Alkhatib, A., &Tsigaris, P. (2020). Spam Emails in Academia: Issues and Costs. Science.

Wangen, G., et al. (2017). An Empirical Study of Root-Cause Analysis in Information Security Management. Conference Proceedings.

Compton, Y. R. (2020). Data Security Obstacles and Strategies from Carolina Universities. Walden University Thesis.

Rahman, N. A. A., Sairi, I. H., & Zizi, N. A. (2020). Challenges of Implementing Cybersecurity Education in Schools. International Journal of Information and Education Technology.

Yue, C. (2016). Teaching Computer Science with Cybersecurity Education Built-In. USENIX ASE.

Salamzada, K., Zarina, Z., & Bakar, M. A. (2015). Framework for Security Strategy for Developing Countries. Asia-Pacific Journal of Information Technology and Multimedia.

Ulven, J. B., & Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. Future Internet, MDPI.

Bisho, M. (2017). Cybersecurity Curricular Guidelines. Springer International Publishing.

Cuchta, T., et al. (2019). Human Risk Factors in Cybersecurity. SIG Conference on Information Education.

Arianto, A. and Anggraini, G. (2019). Building Indonesia's national cyber defense and security to deal with global cyber threats through the Indonesia Security Incident Response Team on Internet Infrastructure (id-sirtii). Journal of Defense & National Defense, 9(1), 13. https://doi.org/10.33172/jpbh.v9i1.497

Faizal, M. (2023). Information technology risk analysis in Islamic banks: identification of the latest threats and challenges. Journal of Ash-Shariah Journal of Islamic Economic and Business Financial Institutions, 5(2), 87-100. https://doi.org/10.47435/asy-syarikah.v5i2.2022

Islami, M. (2018). Challenges in the implementation of Indonesia's national cybersecurity strategy are reviewed from the global cybersecurity index assessment. Society of Telematics and Information Research Journal of Information and Communication Technology, 8(2), 137. https://doi.org/10.17933/mti.v8i2.108

Luthfah, D. (2023). Strengthening cybersecurity in Indonesia's financial services sector. Journal of Research and Scientific Works, Research Institute, Trisakti University, 259-267. https://doi.org/10.25105/pdk.v9i1.18643

Triyanto, T. (2020). Opportunities and challenges of character education in the digital era. Journal of Civics Media Citizenship Studies, 17(2), 175-184. https://doi.org/10.21831/jc.v17i2.35476

(2023). Analysis of cybersecurity awareness in e-court application users in court environments. Scientific Journal of Binary Stmik Bina Nusantara Jaya Lubuklinggau, 5(2), 101-107. https://doi.org/10.52303/jb.v5i2.106

Apriadi, D. (2023). Training on the use of e-learning as a learning medium to improve the competence of lecturers at the Faculty of Social and Political Sciences, Musi Rawas University. Journal of Indonesian Community Service, 3(4), 1219-1224. https://doi.org/10.54082/jamsi.834

Arianto, A. and Anggraini, G. (2019). Building Indonesia's national cyber defense and security to deal with global cyber threats through the Indonesia Security Incident Response Team on Internet Infrastructure (id-sirtii). Journal of Defense & National Defense, 9(1), 13. https://doi.org/10.33172/jpbh.v9i1.497

Basri, I., Muliasari, N., &Gurendrawati, E. (2021). Factors that affect the reliability and timeliness of financial reporting in the East Jakarta SKPD. Journal of Accounting for Taxation and Auditing, 2(3), 470-495. https://doi.org/10.21009/japa.0203.01

Faizal, M. (2023). Information technology risk analysis in Islamic banks: identification of the latest threats and challenges. Journal of Ash-Shariah Journal of Islamic Economic and Business Financial Institutions, 5(2), 87-100. https://doi.org/10.47435/asy-syarikah.v5i2.2022

Hadiprakoso, R. and Satria, W. (2022). Design and build gamification applications to increase cybersecurity awareness. Scientific Journal of Computer Science, 8(2), 94-100. https://doi.org/10.35329/jiik.v8i2.232

Juaningsih, I., Hidayat, R., Aisyah, K., & Rusli, D. (2021). The reconception of the supervisory agency related to the protection of personal data by corporations as an enforcement of the right to privacy based on the constitution. Salam Journal of Social and Cultural Syar I, 8(2), 469-486. https://doi.org/10.15408/sjsbs.v8i2.19904

Luthfah, D. (2023). Strengthening cybersecurity in Indonesia's financial services sector. Journal of Research and Scientific Works, Research Institute, Trisakti University, 259-267. https://doi.org/10.25105/pdk.v9i1.18643

Satrio, J., Maryam, S., Ummah, A., & Wahidin, D. (2022). Improving cybersecurity skills for the manager of the Baros Village site in Serang Regency. Journal of Community Service and Empowerment Innovation, 2(2), 135-142. https://doi.org/10.54082/jippm.35

Sussolaikah, K. (2023). Cybersecurity awareness education media training at sdn 01 Pandean, Madiun City. Abdimas Science and Technology, 3(2), 131. https://doi.org/10.53513/abdi.v3i2.8749

Waskita, A. (2023). Indonesian cyber diplomacy in the implementation of capacity building on national cybersecurity strategy workshop 2019. Padjadjaran Journal of International Relations, 5(2), 142. https://doi.org/10.24198/padjir.v5i2.41337