Cyber Resilience to Digital Threats for Education Institutions 4.0

Budi Wibowo
Department of Informatics Engineering, Institut Teknologi Budi Utomo Jakarta, Indonesia

Andrie Yuswanto
Department of Informatics Engineering, Institut Teknologi Budi Utomo Jakarta, Indonesia

Taufik Hidayat
Department of Computer Engineering, Universitas Indonesia, Indonesia

Nadim Ibrahim
Department of CSE, Arab International University, Damascus, Syria

Abstract: The emergence of Education 4.0, characterized by personalized learning, smart technologies, and digital interconnectivity, has revolutionized academic environments. However, this digital transformation has simultaneously increased the exposure of educational institutions to sophisticated cyber threats. This research addresses the pressing need for a robust cyber resilience framework tailored to the education sector. Employing a qualitative descriptive methodology, supported by secondary data analysis and case study reviews, the study identifies core vulnerabilities in digital infrastructure, policy shortcomings, and a general lack of cybersecurity awareness among stakeholders. In response, the paper proposes a contextualized cyber resilience framework grounded in layered security principles, zero-trust architecture, and institution-wide digital hygiene initiatives. Key findings indicate that effective cyber resilience in Education 4.0 must be multidimensional, incorporating stringent policy enforcement, continuous digital skills training, and adaptive technological strategies. The primary contribution of this study lies in offering a practical, scalable framework that aligns cybersecurity practices with the evolving demands of digital education. Future research is encouraged to explore real-time implementation metrics, cross-institutional collaborations, and the integration of AI-driven threat detection systems to further strengthen educational cyber resilience.

Correspondents Author:
Budi Wibowo, Department of Informatics Engineering, Institut Teknologi Budi Utomo Jakarta, Indonesia
Email: budiwibowo1993@gmail.com

Received: May 13, 2025; Revised June 11, 2025; Accepted: June 12, 2025; Publication: June 17, 2025

Keywords: Cyber resilience, Education 4.0, digital threats, zero trust, information security in education

Introduction

The global education sector is currently undergoing a significant transformation in response to the Fourth Industrial Revolution (4IR), often referred to as Education 4.0. This concept emphasizes the integration of smart technologies, automation, artificial intelligence (AI), and data-driven systems into educational environments (Mourtzis et al., 2022). It not only reshapes the teaching and learning process but also transforms how institutions are managed and how educational services are delivered. Education 4.0 highlights the importance of flexibility, personalized learning, and the digital optimization of both teaching and administrative function (Joshi et al., 2024). In Indonesia, the implementation of digital ecosystems in higher education has been accelerated through national initiatives such as the Merdeka Belajar Kampus Merdeka (MBKM) program, which encourages innovation, remote learning, and the adoption of adaptive technologies within academic. However, the growing reliance on digital platforms also introduces new risks (Ulven & Wangen, 2021). Cyber threats targeting educational institutions have surged, with universities becoming prime targets due to the vast amounts of sensitive data they store from personal information and intellectual property to financial records (Velusamy, 2025). Common attacks include phishing, ransomware, data breaches, and denial-of-service (DoS) attacks. In Southeast Asia, cyberattacks on universities have risen by up to 45% since the onset of the COVID-19 pandemic, following the abrupt shift to online systems. Educational institutions, especially those with limited cybersecurity infrastructure and low awareness, have become increasingly vulnerable to complex digital threats that can disrupt operations (Cheng & Wang, 2022). In Indonesia, cyber incidents in the education sector are becoming more frequent, though many remain unreported. Studies indicate that numerous institutions lack adequate cybersecurity policies, suffer from weak governance structures, and have insufficient technical protections in place. This problem is particularly acute in small and medium-sized private universities, where budget constraints hinder the development of robust information security systems and the recruitment of professional IT personnel. Low cybersecurity literacy among students, faculty, and even institutional leaders further amplifies the risks associated with digital transformation (Ozkan-okay et al, 2023).

This situation underscores the importance of building cyber resilience the institution's ability to anticipate, withstand, respond to, and recover from cyber incidents while maintaining core operations. Cyber resilience goes beyond traditional preventive approaches, focusing instead

on an organization's adaptive capacity through technical, human, and procedural measures (Annarelli & Palombi, 2021). In the education context, this means embedding resilience into IT systems, staff training, institutional policies, and decision-making processes. Previous research has explored cybersecurity and resilience in academic environments (Tzavara & Vassiliadis, 2024) highlighted the role of institutional leadership in fostering a culture of cybersecurity awareness. (Andronache, 2021) assessed the vulnerabilities of cloud-based academic systems and recommended secure-by-design principles. Other studies advocate integrating cybersecurity literacy into university curricula as a long-term resilience strategy (El-Hajj et al., 2024). However, most of these studies focus on large institutions or solely on technical aspects such as network architecture and data encryption (Fikri et al., 2022). Unfortunately, comprehensive studies on cyber resilience in Indonesian private universities remain limited. Empirical data reflecting institutional preparedness for digital threats particularly in resource-constrained environments are scarce. Furthermore, case-based research that views cyber resilience as an organizational and cultural issue, rather than a purely technical one, is rare. Without a holistic understanding of the interplay between human behavior, institutional policies, and technology, resilience-building efforts risk being ineffective. This study seeks to fill that gap by examining the state of cyber resilience at Campus X, a private university in Jakarta that actively adopts digital learning platforms, online administrative systems, and remote services. While the institution appears to be transitioning toward the Education 4.0 model, initial observations suggest that its security governance is not yet fully developed (Wan Norhayate et al., 2023). The university lacks formal cybersecurity policies, conducts infrequent risk assessments, offers limited awareness training, and has minimal investment in digital These factors make Campus X a relevant case study for exploring the real-world challenges of building cyber resilience in Indonesia's private higher education sector. Theoretically, this research contributes to the development of a contextual cybersecurity resilience framework tailored to the characteristics of mid-sized educational institutions. It explores the interplay between technical measures, organizational readiness, and user behavior, aligning with resilience theory that emphasizes adaptive capacity over mere threat prevention (Verma et al., 2025). Practically, the findings offer valuable insights into institutional leaders and policymakers to design effective and resource-conscious resilience strategies. The urgency of this study is underscored by post-pandemic trends that promote hybrid and online learning models, which increase dependence on digital systems (Cheng & Wang, 2022b). Without adequate cyber resilience, even minor incidents can disrupt educational continuity, endanger student data, and erode public trust in institutions. In an era driven by data and AI, the security and integrity of information have

become foundational to quality assurance in education. Therefore, this study aims to assess the cyber resilience capacity of Campus X as a representation of digitally transforming private universities in Indonesia. Its primary objective is to identify strengths and weaknesses in the campus' cybersecurity practices, analyze organizational and behavioral factors that influence resilience, and provide strategic recommendations for improvement. By doing so, the study not only enriches theoretical discourse on cyber resilience in education but also offers practical guidance to enhance institutional preparedness in the era of Education 4.0.

Research Method

This study employs a qualitative approach using a descriptive method to gain an in-depth understanding of cyber resilience in private educational institutions undergoing transformation towards Education 4.0. This approach is chosen as it is well-suited to explore complex socio-technical phenomena, including the interaction between institutional policies, technical preparedness, and user behavior. This research was conducted at Campus X, a private university in Jakarta that has adopted various digital systems in its teaching and administrative processes. The site was selected purposely, based on the institution's active engagement in digital transformation, yet with indications of weak information security governance. Data collection was carried out using three main techniques: semi-structured interviews with IT managers, lecturers, and administrative staff to explore cybersecurity practices within the institution; direct observation of the campus's information technology systems, including the Learning Management System (LMS), online attendance systems, and network infrastructure; and document analysis involving reviews of IT security policies, digital standard operating procedures (SOPs), incident reports (if available), and data management policies. The instruments used in this study consisted of interview guides and observation sheets developed based on the cybersecurity resilience framework from the National Institute of Standards and Technology (NIST) and the principles of Zero Trust architecture. In addition, supporting tools such as Google Forms and digital note-taking applications were utilized to assist in the data collection and tracking process. The data analysis technique applied was thematic analysis, which involved several stages: data reduction to extract key information from interviews, observations, and documents; theme categorization based on dimensions of cybersecurity resilience such as policy, technology, and user literacy; source triangulation to compare findings from various data collection methods in order to enhance validity; and interpretation to draw meaning and patterns from the data, linking them to relevant literature and theories. Campus X was purposely selected as it represents a medium-sized private university with approximately 4800 students and a moderate level of digital maturity. The

institution has implemented core digital systems such as an LMS, and e-administration yet lacks advanced cybersecurity governance structures. This combination makes it a suitable subject for exploring the challenges faced by digitally transitioning institutions with limited resources.

Results and Discussion

The findings of this study reveal a significant disparity between Campus X's commitment to digital transformation and its ability to manage the accompanying cybersecurity risks. Despite implementing digital systems aligned with the goals of Education 4.0, such as LMS, online attendance, and digital administrative services—the institution lacks robust cybersecurity governance, which renders it highly vulnerable to digital threats. The prevalence of incidents like phishing, credential theft, and unauthorized access, coupled with the absence of a formal incident response protocol, underscores a critical institutional gap in cybersecurity resilience. These findings align with global trends reported in the State of Cyber Security 2025 by check Point, which indicates that the education sector has seen a 75% increase in weekly cyberattacks, making it the most targeted industry. This external data not only validates the experiences observed at Campus X but also situates them within a broader, alarming trend in education sector cybersecurity.

Moreover, this study supports prior research who found that many educational institutions in Southeast Asia underestimate cyber risk due to the misconception that schools are less attractive to cybercriminals. However, institutions like Campus X hold vast amounts of sensitive data (e.g., student records, staff credentials, financial transactions), making them prime targets. The lack of awareness and technical response mechanisms observed in this study reflect what Sharma describes as "digital naïveté" a common issue in digitally transitioning institutions with low cybersecurity maturity. In terms of governance, the findings align with Gordon et al. (2021), who emphasized that cybersecurity readiness in educational institutions is not solely a technical issue but a multidimensional one involving policy, human behavior, and institutional culture. At Campus X, while the technical infrastructure (e.g., LMS, network systems) is in place, the institutional culture remains reactive rather than proactive. For instance, cybersecurity responsibilities are often centralized under the IT division without cross departmental collaboration or regular training, echoing Gordon's warning about siloed approaches to cyber governance. Additionally, this study highlights a misalignment between policy and practice. While some IT security policies exist at Campus X, they are not well disseminated, enforced, or integrated into daily

operational routines. Who identified policy-practice gaps as a major hindrance to effective cyber resilience in Middle Eastern universities undergoing digital transformation.

A noteworthy point from the thematic analysis is the low level of cybersecurity literacy among staff and faculty, which serves as a critical vulnerability. Which argues that user behavior is often the weakest link in organizational cybersecurity, especially in sectors that prioritize educational innovation over digital defense. In sum, the findings of this study demonstrate that while digital transformation efforts are well-intentioned and necessary for alignment with Education 4.0, they must be coupled with integrated, institution-wide cybersecurity frameworks that emphasize: (a) Continuous training and awareness; (b) Clear incident response procedures; (c) Policy enforcement mechanisms; (d) Cross-functional governance models. Without these, institutions like Campus X risk undermining the very digital advancements they seek to implement.

From an institutional perspective, Campus X lacks formal information security policies such as official decrees (SK) or Standard Operating Procedures (SOPs) to govern data and system security. Furthermore, there are no regular security audits or periodic risk assessments in place. The lack of resources also presents a significant obstacle; the IT team is limited, and most of its staff do not have cybersecurity certifications. This impacts the institution's ability to detect and respond to incidents. Digital security literacy is also limited among both students and faculty. Many campus users are found to use weak passwords and access campus systems from insecure devices, which increases the potential security vulnerabilities. Based on this analysis, the study proposes a three-layer cybersecurity resilience model for Education 4.0 institutions, particularly for medium-sized private universities. The first layer is governance and policy, which includes the development of risk-based security policies, the establishment of an incident response team, and the integration of security policies into the institution's strategic plan. The second layer is technology, which encompasses network segmentation, the implementation of multi-factor authentication (MFA), and the use of lightweight artificial intelligence-based anomaly detection systems. The third layer is awareness and culture, which emphasizes cybersecurity literacy training, regular incident simulations, and the integration of cybersecurity topics into the curriculum. This model is adaptive and considers the institution's resource limitations. Its goal is to build internal capacity to detect, respond to, and recover from cyber incidents efficiently without disrupting the learning process. This approach aligns with the view of Alghamdi and Migdadi (2023), who stress the importance of digital literacy as a key pillar of cybersecurity resilience in the education sector. Additionally, Kumar et al. (2022) emphasize that educational institutions must shift from a passive protection paradigm to a resilience approach based on adaptation and sustainability. This

research also extends the findings by highlighting that cybersecurity resilience strategies should be tailored to the organization's conditions, particularly for mid-sized institutions with technical and financial limitations. Without this contextual understanding, efforts to build cybersecurity resilience are at risk of being ineffective or unsustainable. Field data indicates that Campus X has faced various security incidents, including phishing attacks, breaches of internal network access, and malware infections. Over the past two years, six incidents have been recorded, none of which have been systematically addressed due to the lack of formal policies and an emergency response team. This reflects a broader pattern among private universities in Indonesia, where 63% of institutions lack information security policies and only 17% conduct regular security audits . In contrast, universities in countries like Singapore show a stark difference. All public universities there have implemented a zero-trust framework, comprehensive MFA usage, and AI-based systematic audits every six months (MOE, 2022). This highlights the critical importance of building cybersecurity resilience not only through technology but also through governance, human resources training, and strategic investments in digital security.

Based on a questionnaire survey involving 60 respondents from various educational institutions, it was found that, in general, awareness of the importance of cybersecurity resilience is starting to take shape, although there are still weaknesses in its implementation on the ground. In the IDENTIFY category, 92.9% of institutions have a documented inventory of digital assets, and 85% of them have information security policies. This indicates that most institutions recognize the importance of identifying digital resources and the associated risks. However, 7.1% of institutions still lack digital asset inventories, which could represent a potential vulnerability in their security systems. In the PROTECT category, the majority of institutions (92%) have mandated strong password usage for all system users. However, only 51.1% of institutions have implemented two-factor authentication (2FA), indicating that user account protection from unauthorized access remains suboptimal in nearly half of the surveyed institutions. In the DETECT category, 64.3% of institutions report having network security monitoring systems in place. However, 28.6% of respondents indicate that their institution does not have such a system, and 7.1% are unaware of its existence. This shows that although early detection efforts are in place, many institutions still lack adequate visibility into potential cyberattacks. Regarding RESPONSE, 64% of institutions claim to have an incident response team, but 36% do not have a formal structure or procedures for responding to security incidents. The average readiness score for institutions in responding to incidents, based on a 1-5 Likert scale, is 3.9. This indicates that preparedness is at an "adequately ready" level but still requires improvement in both procedures and human resources. Meanwhile, in

the RECOVER category, 64% of institutions report having a recovery plan for systems after incidents, but only 57.1% regularly perform backup and recovery simulations. This means that while recovery plans are in place, their execution is not yet consistently and measurably performed in practice. Overall, the evaluation results indicate that most educational institutions have taken initial steps toward strengthening cybersecurity resilience, especially in terms of identification and basic protection. However, the implementation of advanced technical controls such as 2FA, active threat detection systems, and regular recovery practices still require attention and improvement. To achieve optimal cybersecurity resilience, a comprehensive integration of the NIST Cybersecurity Framework and Zero Trust principles, supported by policies, training, and adequate resource allocation, is necessary. Below is a visualization of the Control-Based Assessment, which illustrates the level of cybersecurity control implementation based on the NIST functions in educational institutions. This diagram highlights strong areas such as password usage and digital asset inventory, as well as areas that still need improvement, such as 2FA and recovery simulations.

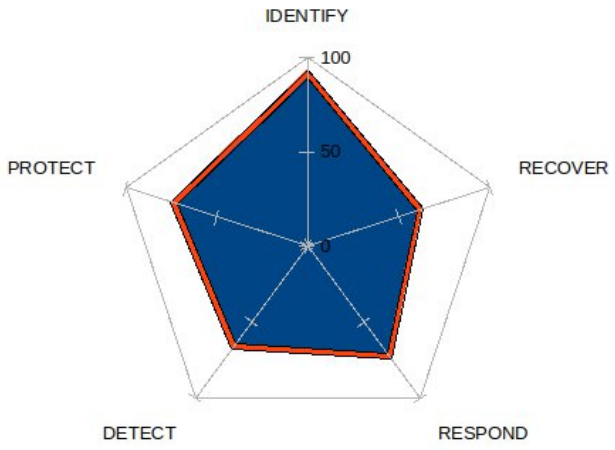

Figure 1 Control-Based Assessment radar diagram based on the NIST Cybersecurity Framework.

Table 1 Summary of Institutional Cyber Resilience Questionnaire Results (n = 60)

NIST Categories	Evaluation Indicator	Y (%)	N (%)	Others
IDENTIFY	The institution has a list of digital assets	92.9	7.1	0% (Don't Know)
IDENTIFY	Information security policy in place	85	14.3	-
PROTECT	Users are required to use strong passwords	92	8	-
PROTECT	Use two-factor authentication (2FA)	51.1	42.9	-
DETECT	Network security monitoring system in place	64.3	28.6	7.1 % (Don't Know)
RESPOND	Has an incident response team	64	36	-

RESPOND	Average readiness to respond to incidents (Likert 1-5)	-	-	3.9
RECOVER	Have a system recovery plan	64	36	-
RECOVER	Conduct periodic backup/restore simulations	57.1	42.9	

The evaluation of 60 educational institutions shows that there is generally an initial awareness of the importance of cyber resilience, particularly in terms of digital asset identification and the implementation of basic security policies. However, more in-depth implementations such as the use of two-factor authentication (2FA), threat detection systems, and periodic recovery and simulation practices are still uneven and not optimized. This unpreparedness shows that many institutions are still at an early stage in building a robust and sustainable security system. To strengthen cyber resilience in the Education 4.0 era, institutions need to adopt a more comprehensive approach, based on the NIST framework and Zero Trust principles, and improve human resource capacity, infrastructure and information security policies that support effective incident response and recovery. To further support institutional decision-making, a basic cost-benefit consideration of Multi-Factor Authentication (MFA) implementation was analyzed. While MFA adoption may require initial investment in authentication tools and user onboarding, its benefits in reducing account compromise rates and ensuring data integrity significantly outweigh the costs. Studies have shown that MFA can reduce unauthorized access by up to 99%, leading to lower recovery costs and reduced downtime, which are crucial for maintaining educational continuity.

Conclusions

This study is focused on a single private university in an urban setting, which may limit the generalizability of the findings. Vocational schools or institutions in rural or non-urban areas may face different infrastructural constraints and user literacy profiles. Future research should explore multiple case studies across diverse geographic and institutional types to validate and refine the proposed resilience framework under varying conditions. Digital transformation in the context of Education 4.0 opens up great opportunities for educational institutions to improve efficiency, accessibility and innovation in the learning process. However, along with this progress comes serious challenges in the form of increasingly complex digital security threats. The results of the case study on Campus X show that cyber resilience has not been a top priority, as reflected in the absence of formal policies, lack of cyber awareness training, and underinvestment in digital security infrastructure. Cyber resilience not only demands technical solutions such as double authentication and firewalls, but also requires strong governance, a supportive organizational culture, and digital literacy

across campus elements. The three-layer model proposed in this research covering policy, technology and awareness can be an initial framework for building cyber resilience in secondary private educational institutions. This approach is adaptively designed to remain relevant despite budget and human resource constraints. By adopting a strategic and holistic approach, educational institutions can increase resilience to digital threats while maintaining the sustainability of educational services in the digital era.

References

Andronache, A. (2021). Increasing security awareness through lenses of cybersecurity culture. *Journal of Information Systems & Operations Management*, *15.1*(July), 7–23.

Annarelli, A., & Palombi, G. (2021). Digitalization capabilities for sustainable cyber resilience: a conceptual framework. *Sustainability (Switzerland)*, *13*(23). https://doi.org/10.3390/su132313065

Cheng, E. C. K., & Wang, T. (2022a). Estrategias Institucionales para la Ciberseguridad en la Educación Superior Instituciones educativas. *Information (Switzerland)*, *13*(4), 1–14.

Cheng, E. C. K., & Wang, T. (2022b). Institutional Strategies for Cybersecurity in Higher Education Institutions. *Information (Switzerland)*, *13*(4). https://doi.org/10.3390/info13040192

El-Hajj, M., Itäpelto, T., & Gebremariam, T. (2024). Systematic literature review: Digital twins' role in enhancing security for Industry 4.0 applications. *Security and Privacy*, *7*(5), 1–37. https://doi.org/10.1002/spy2.396

Fikri, A. M., Atrinawati, L. H., & Putra, M. G. L. (2022). Cyber Resilience Evaluation Using Cyber Resilience Review Framework at University XYZ. *International Journal of Educational Management and Innovation*, *3*(2), 155–168. https://doi.org/10.12928/ijemi.v3i2.5794

Hausken, K. (2020). Cyber resilience in firms, organizations and societies. *Internet of Things (Netherlands)*, *11*, 1–9. https://doi.org/10.1016/j.iot.2020.100204

Joshi, K., Kumar, R., Bharany, S., Saini, D. K. J. B., Kumar, R., Ibrahim, A. O., Abdelmaboud, A., Nagmeldin, W., & Medani, M. A. (2024). Exploring the Connectivity between Education 4.0 and Classroom 4.0: Technologies, Student Perspectives, and Engagement in the Digital Era. *IEEE Access*, *12*(January), 24179–24204. https://doi.org/10.1109/ACCESS.2024.3357786

Mourtzis, D., Panopoulos, N., & Angelopoulos, J. (2022). A hybrid teaching factory model towards personalized education 4.0. *International Journal of Computer Integrated Manufacturing*, *36*(12), 1739–1759. https://doi.org/10.1080/0951192X.2022.2145025

Ozkan-okay, M., Yilmaz, A. A., Akin, E., Aslan, A., & Aktug, S. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, *Electronics*, *12*(1333).

Tzavara, V., & Vassiliadis, S. (2024). Tracing the evolution of cyber resilience: a historical and conceptual review. *International Journal of Information Security*, *23*(3), 1695–1719. https://doi.org/10.1007/s10207-023-00811-x

Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education-Una revisión sistemática de los riesgos de ciberseguridad en Educación más alta. *Future Internet*, *13*(2), 1–40.

Velusamy, G. (2025). *Enhancing Cybersecurity in Educational Institutions: Challenges and Strategies*. *February*.

Verma, P., Newe, T., O'Mahony, G. D., Brennan, D., & O'Shea, D. (2025). Towards a Unified Understanding of Cyber Resilience: A Comprehensive Review of Concepts, Strategies, and Future Directions. *IEEE Access*, *13*(February), 49945–49965. https://doi.org/10.1109/ACCESS.2025.3551887

Wan Norhayate, W. D., Dioubate, B. M., Fakhrul Anwar, Z., Fauzilah, S., Mohd Faiz, H., & Ooi Hai, L. (2023). Securing Higher Education Institutions in the Fourth Industrial Revolution: Developing a Cybersecurity Risk Management Framework in Malaysia. *Communications of International Proceedings*, *2023*. https://doi.org/10.5171/2023.4116023