

Cybersecurity Law and Risk Management in Technology-Enhanced Learning Factories

Imam Rahmaddani^{1*} 

¹Faculty of Law, Islamic University of Syekh Yusuf, Indonesia

¹irahmaddani@unis.ac.id

*Corresponding Author

Article Info

Article history:

Submission May 28, 2026

Revised June 22, 2026

Accepted September 19, 2026

Published September 29, 2026

Keywords:

Cybersecurity Law

Risk Management

Learning Factory

Legal Compliance

Data Protection



ABSTRACT

Higher education institutions increasingly operate technology enhanced learning factories that connect instructional platforms to real or simulated production equipment. This arrangement enlarges the attack surface of academic networks and introduces legal obligations that conventional campus policies do not cover. **This study** investigates cybersecurity exposure in higher education and the legal and risk management obligations of institutions that operate such facilities, with Indonesia as the primary jurisdiction. **A qualitative** literature review and a doctrinal analysis of Indonesian statutes were combined with a secondary analysis of the Verizon Data Breach Investigations Report 2024, the Sophos State of Ransomware in Education 2024 survey, and reports of the National Cyber and Crypto Agency (Badan Siber dan Sandi Negara, BSSN) for 2021 to 2024. The data show 1,537 confirmed breaches among 1,780 education incidents in 2024, an increase in ransomware encryption in higher education from 73 percent to 77 percent, and a mean recovery cost of USD 4.02 million. **On this basis**, the study proposes a four layer awareness framework and a Legal Risk Governance model that treats legal duties as risk acceptance criteria and favors controls that preserve experimental learning. Both proposals are aligned with Sustainable Development Goals 4, 9, and 16 and with Indonesian regulation. **The findings** provide institutions with a structured basis for governing open learning environments without leaving unlawful residual risk.

This is an open access article under the [CC BY 4.0](https://creativecommons.org/licenses/by/4.0/) license.



DOI: <https://doi.org/10.33050/itee.v5i1.1143>

This is an open-access article under the CC-BY license (<https://creativecommons.org/licenses/by/4.0/>)

©Authors retain all copyrights

1. INTRODUCTION

Universities depend on digital systems for teaching, administration, and research. Learning Management Systems (LMS), student records, research repositories, and cloud services are now accompanied, in some institutions, by Technology Enhanced Learning Factories (TELFs). A TELF connects instructional software to real or simulated production equipment, so that students work with Programmable Logic Controllers (PLCs), sensors, Internet of Things (IoT) interfaces, digital twins, and process data supplied by industry partners [1, 2]. A Higher Education Institution (HEI) that operates such a facility is therefore responsible for two environments at the same time. One is an educational setting populated by novice users, and the other is a small industrial plant built on Operational Technology (OT).

This dependence has been accompanied by a marked increase in exposure. The Verizon Data Breach Investigations Report (DBIR) 2024 recorded 1,780 security incidents in the education sector, of which 1,537

were confirmed data breaches [3]. The Sophos State of Ransomware in Education 2024 survey, which gathered responses from 600 Information Technology (IT) and cybersecurity leaders in 14 countries, reports that data were encrypted in 77 percent of ransomware attacks on higher education in 2024, compared with 73 percent a year earlier. The mean recovery cost rose from USD 1.06 million to USD 4.02 million over the same period [4]. The DBIR further reports that 68 percent of breaches across all sectors involved a nonmalicious human element, that is, an error or a successful social engineering attempt [3].

The Indonesian situation shows a different but equally serious pattern. The National Cyber and Crypto Agency (Badan Siber dan Sandi Negara, BSSN), recorded 1,637,973,022 traffic anomalies in 2021, 976,429,996 in 2022, and 403,990,813 in 2023. Of the 2023 total, 1,011,209 were classified as ransomware activity and 4,001,905 as Advanced Persistent Threat (APT) activity [5]. The aggregate count declined, whereas the severity of individual incidents increased. In June 2024, a ransomware attack on the Temporary National Data Center (Pusat Data Nasional Sementara, PDNS), the temporary national data center in Surabaya, disrupted government services nationwide [6, 7]. EDUCAUSE ranked cybersecurity first among its 2026 Top 10 IT issues and framed it as a responsibility shared across the campus community [8].

Legal exposure adds a further dimension. Indonesia's Personal Data Protection Law (Law No. 27 of 2022; UU PDP) imposes duties on controllers and processors of personal data, and a TELF holds learner identities, performance records, access logs, and, in some designs, biometric signals from wearable devices [9]. Industry partners also deposit confidential process knowledge in the same facility. Existing studies generally position industrial laboratories and blockchain based record systems as instruments of instruction or as technical safeguards [10, 11]. Comparatively few studies examine the operated TELF as a regulated object whose operator is answerable simultaneously for learner data protection and for the safety of physical processes.

The present study addresses this gap through three research questions. The first concerns the scale, cost, and trajectory of cyber threats to higher education according to current global and Indonesian data. The second concerns the legal duties that fall on an institution operating a TELF and the manner in which those duties interact with the facility's architecture. The third concerns the form of a governance and awareness framework that can reconcile those duties with the open character of a learning factory. The study contributes a layered reference architecture for the TELF, an actor and duty matrix derived from Indonesian law, a mapping of threat classes to controls that preserve pedagogical openness, a four layer awareness framework, and a Legal Risk Governance model for TELF (LRG-TELF). The proposals are aligned with Sustainable Development Goals (SDG) 4, 9, and 16 and with Indonesian regulation.

2. LITERATURE REVIEW

The relevant literature is organized into five areas. These are the global threat profile of universities, the Indonesian national context, the TELF as a cyber physical educational system, the legal and standards basis for risk management, and the human dimension of awareness.

2.1. Cybersecurity Threat Landscape and TELF Exposure

Universities combine large numbers of loosely governed endpoints with sensitive research and personal data [11]. The DBIR reports that ransomware and other forms of extortion featured in 32 percent of all breaches in 2024 and ranked among the three most frequent threat actions in 92 percent of industries [3]. Exploitation of vulnerabilities as the initial step of a breach almost tripled to 14 percent of breaches, and a further 15 percent involved a third party such as a software supplier. Education was the first sector affected by the MOVEit file transfer campaign, which subsequently extended to finance and insurance [3]. Human factors are as consequential as software flaws. Errors alone accounted for 28 percent of breaches, and the broader nonmalicious human element for 68 percent.

The DBIR does not publish a separate education-sector distribution of internal and external actors. In universities, the relevant patterns are accidental insider error, malicious privilege misuse, external social engineering, and externally initiated system intrusion; these are interpretive categories rather than sector-specific DBIR statistics. In universities, insider risk is often accidental, while ransomware and system intrusion are commonly externally initiated. These patterns can connect into a single incident from initial compromise to institutional impact. A common attack path begins with phishing or exploitation of an unpatched service, followed by lateral movement, privilege escalation, and ransomware or data theft. In a TELF, IoT-OT interfaces and remote or hybrid access add entry points that conventional academic networks do not possess [4, 12]. The proposed framework therefore addresses the attack sequence rather than a single control.

BSSN coordinates national cybersecurity through its National Security Operations Center, which monitors traffic anomalies across government and strategic sector networks [5]. The decline in anomaly counts between 2021 and 2023 requires cautious interpretation. BSSN attributes part of the decline to refinements in detection methods and points to a shift toward more sophisticated threats, including backdoor communications by remote access trojans [5]. The PDNS incident of 2024 demonstrated that public digital infrastructure remains exposed even when aggregate counts decrease [6, 7].

At the level of individual behavior, the 2024 National Cybersecurity Awareness Survey (Survei Kesadaran Keamanan Siber, SKKS) covered 8,511 secondary school respondents across 34 provinces. The resulting Cybersecurity Awareness Index (Indeks Kesadaran Keamanan Siber, IKKS) showed that respondents were mostly within the Good to Very Good range, although weaknesses remained in incident reporting and personal data sharing practices [13]. These students will enter universities within a few years, which makes the findings relevant to HEIs despite the younger age of the sample.

Learning factories are teaching environments that reproduce production conditions so that students can develop competencies on real equipment [1]. Educational information systems designed for learning factory management in HEIs place the LMS and assessment services above manufacturing execution, digital twin, and data historian layers, while remote laboratories and partner portals extend beyond the campus perimeter [2]. Technology enhancement therefore increases the number of relationships among learners, instructors, technicians, industry partners, and cloud or OT vendors.

Fig. 1 presents the reference architecture adopted in this study. The architecture runs from the physical cell and the edge controllers, through the industrial network and the Manufacturing Execution System (MES) with its digital twin, to the LMS with assessment analytics, and finally to remote and hybrid access for partners and vendors. Data flow continuously across these layers. Machine telemetry moves upward for simulation and assessment, while instructional set points and firmware move downward. A failure of confidentiality, integrity, or availability at any layer may consequently disrupt both learning activities and legal compliance.

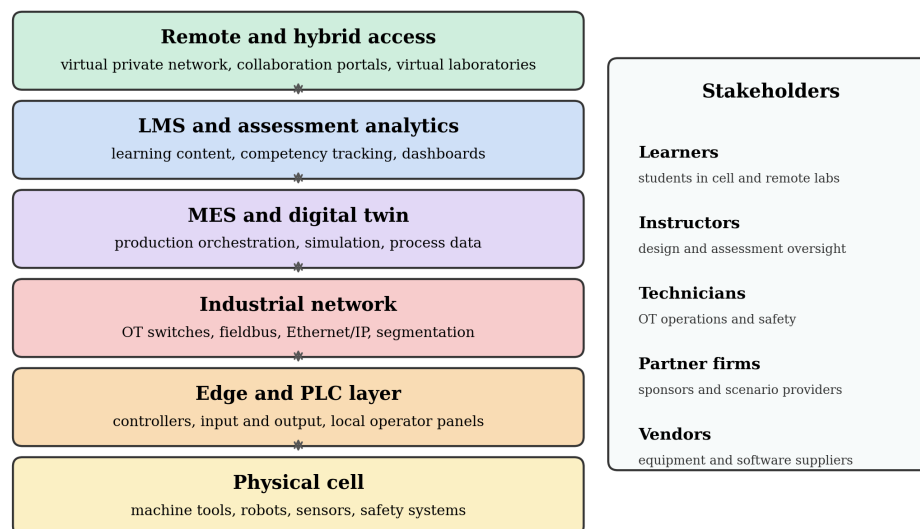


Figure 1. Layered reference architecture of a TELF with stakeholder roles. The diagram is a conceptual construct and does not depict a measured deployment.

Three characteristics distinguish a TELF from other facilities and bear directly on governance. First, unlike a sealed computer laboratory, a TELF contains actuators capable of causing injury or interrupting a process. Second, unlike a production plant, its primary mission is learning, so temporary accounts, exploratory configurations, and assessment telemetry are routine and not exceptional. Third, industry sponsorship places confidential process knowledge inside an educational setting, an exposure that blockchain based intellectual property designs seek to address [14]. Governance models for blockchain integrated IoT ecosystems assist in defining accountability boundaries between OT and IT without reducing a TELF to either a plant or a classroom [15]. Cybersecurity guidance for manufacturing in Industry 4.0 remains applicable to perimeter and remote

access design [12].

Studies of manufacturing security describe ransomware directed at OT, lateral movement from IT networks, insecure remote access, and compromised firmware in the supply chain [12, 16]. Research on the integration of IoT and blockchain shows that telemetry and business data become shared targets for theft and tampering [17]. Risk analyses from the financial sector catalogue threat classes and mitigation approaches that can be transferred to teaching settings once filtered for pedagogical purposes [18].

A TELF inherits these risks and adds risks of its own. Learner cohorts turn over rapidly and reuse shared operator stations and project repositories, which weakens accountability. The pedagogical need for students to observe and occasionally modify control logic conflicts with the principle of least privilege. Remote and hybrid laboratories extend the attack surface beyond the campus. Learning analytics and wearable or biometric streams concentrate sensitive personal data, and their misuse harms both privacy and assessment integrity [11, 19]. Records of grade and internship conversion show that assessment data constitute an integrity object requiring protection in its own right [20].

Insider actions may be accidental, for example through incorrectly wired controller logic, or opportunistic, such as the copying of a partner's design files. Attacks on assessment pipelines reduce trust in academic credentials even when the physical plant remains safe, and studies of secure authentication and online examination platforms describe the structure of these pipelines [21, 22]. Availability failures during peak assessment periods produce academic and reputational costs that industrial risk registers seldom record. Educational testbeds built to teach industrial security exhibit the same weaknesses from a didactic perspective, and the host institution should treat them as production risks whenever real learners, partner data, or actuators are involved. Blockchain studies of campus held records support the same conclusion for academic data [10, 23].

2.2. Legal, Risk Governance, and Human Factors

The TELF is treated here as a regulated processing environment, not merely a technical laboratory. Under Indonesia's Personal Data Protection Law (UU PDP), learner identities, access logs, assessment records, and biometric data fall within personal-data governance [9]. For TELF operators, the most material provisions are: data-protection impact assessment for high-risk processing (Art. 34); security of processing and organizational safeguards (Arts. 35–39); written breach notification within 3 x 24 hours where Art. 46 applies; and controller accountability under Art. 47. These duties mean that a cybersecurity failure can become legal non-compliance even when teaching operations continue. The UU ITE, as amended by Law No. 1 of 2024, supplies the electronic-systems layer of the framework [24]. Perpres 82/2022 defines vital information infrastructure around electronic systems using information technology and/or operational technology whose disruption may seriously affect public interests, public services, national security, or the economy [25]. A TELF is not automatically designated as vital information infrastructure; this study therefore uses Perpres 82/2022 as an infrastructure-risk benchmark rather than claiming statutory designation. This distinction strengthens doctrinal accuracy while recognizing the IT/OT convergence shown in Fig. 1.

The resulting legal rule for LRG-TETF is strict: legal duties operate as risk-acceptance constraints. A residual risk may be technically below institutional appetite yet remain unacceptable if purpose limitation, security, unauthorized-access prevention, breach notification, accountability, or contractual confidentiality duties are not satisfied. ISO/IEC 27005:2022 organizes information security risk management into context establishment, identification, analysis, evaluation, treatment, and monitoring [26]. ISO/IEC 27001:2022 provides the management system within which these activities operate [27, 28]. The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) 2.0 groups outcomes into six functions, namely Govern, Identify, Protect, Detect, Respond, and Recover [29]. None of these documents was written specifically for a TELF, although their underlying logic can be adapted to one.

Compliance oriented risk models developed for payment platforms demonstrate how statutory duties can be encoded as acceptance criteria during treatment selection [30], and the same approach is suitable for a facility bound by UU PDP and UU ITE. Frameworks for blockchain security and privacy inform integrity and non repudiation controls for gradebooks and experiment logs [31]. The extent to which such controls are adopted on campus depends on the organizational factors identified in research on information system governance in HEIs [32] and on the climate established by management [33]. Cybersecurity awareness comprises the knowledge, attitudes, and behaviors that shape how individuals use digital systems, including password practice, phishing recognition, and care with personal data [11, 34]. A cybersecurity culture framework applied to technical attack techniques shows that culture can be assessed alongside technical risk [35]. Because most

breaches continue to involve a human element [3], awareness activities need to be continuous. EDUCAUSE likewise repositions cybersecurity from a purely technical function to a responsibility embedded in everyday workflows [8]. The DBIR offers a practical reference point. In simulated phishing exercises, 20 percent of users reported the message, and 11 percent of those who clicked also reported it [3]. Suitable program metrics therefore include click and report rates, training completion by role, and a periodic knowledge, attitude, and behavior score comparable to the IKKS [13]. Simulated phishing with immediate feedback and short training modules are plausible formats for universities, although evidence on gamified delivery in this population remains limited.

3. RESEARCH METHODOLOGY

This study employs a qualitative literature review combined with a doctrinal analysis of Indonesian legal instruments and a secondary analysis of publicly available cybersecurity statistics. The review follows thematic, evidence based procedures commonly applied in education technology and information systems research. The results were then formulated as obligation and control mappings and as a governance model. No survey or penetration test data were collected, and all constructs presented in the results are qualitative and normative.

3.1. Data Sources and Selection

Three categories of material were used. The first comprises scholarly articles and conference papers published between 2021 and 2026 on cybersecurity, information system protection, learning factories, and educational data protection. These were retrieved from Scopus, Web of Science, IEEE Xplore, and Google Scholar and through citation tracking. Records were screened by title and abstract and subsequently by full text. Opinion pieces, vendor white papers without disclosed methods, and studies outside education or industrial settings were excluded [36]. The second category comprises figures from four named sources, listed in Table 1. The third category comprises legal and standards documents, namely UU PDP, UU ITE, Perpres 82/2022, ISO/IEC 27001 and 27005, and NIST CSF 2.0.

Table 1. Statistical Data Sources Used in This Study

Source	Scope	Reporting Period
Verizon DBIR 2024 [3]	30,458 global security incidents and 10,626 confirmed breaches across 94 countries	Nov. 2022 to Oct. 2023
Sophos State of Ransomware in Education 2024 [4]	600 IT and cybersecurity leaders in 14 countries, education sector	Jan. to Feb. 2024
BSSN cybersecurity landscape reports [5, 6]	National traffic anomaly monitoring and reported major incidents	2021 to 2024
BSSN SKKS [13]	8,511 respondents in 34 provinces, national awareness index	2024

Table 1 shows that the four sources differ considerably in scope and unit of analysis, ranging from global multi sector breach forensics to a single country awareness survey. For this reason, the sources were analyzed in parallel and compared only where their periods and themes overlapped. No pooled statistic was derived from them.

3.2. Doctrinal Analysis and Framework Construction

The doctrinal analysis used statute-to-system mapping. Provisions of UU PDP, UU ITE, and Perpres 82/2022 were classified by legal subject, protected object, operative duty, triggering event, and required institutional response, then mapped to TELF actors and architectural layers. Threat classes were paired with NIST CSF 2.0 functions and pedagogy-preserving controls. LRG-TELF treats mandatory statutory and contractual duties as risk-acceptance constraints: technically tolerable residual risk cannot be accepted when a mapped legal duty remains unsatisfied.

4. RESULTS AND DISCUSSION

The data indicate a persistently high rate at which education incidents become breaches, a marked deterioration of ransomware outcomes in higher education, and an Indonesian threat profile that is smaller in volume but greater in consequence. The legal analysis adds a set of duties that a TELF operator cannot disregard. Because the statistical sources differ in geographic scope, sampling unit, and period, the figures are interpreted source by source. Where two sources are discussed together, the purpose is to compare direction of change, and their absolute values are not treated as equivalent or additive.

4.1. Cybersecurity Exposure and Threat Evidence

The 2024 DBIR recorded 1,537 confirmed education breaches from 1,780 incidents, an incident-to-breach ratio of approximately 86.4 percent. This is a coarse exposure indicator rather than a maturity score. Open university architectures, in which students, faculty, staff, and external partners require broad access, increase the number of identities, endpoints, and trust relationships that must be governed. BSSN traffic anomalies declined from 1.64 billion in 2021 to 976 million in 2022 and 404 million in 2023; BSSN also reported more than one million ransomware-related and nearly four million APT-related anomalies in 2023. This decline should not be interpreted as a proportional reduction in risk. BSSN attributes part of the change to refinements in detection and reports that more than one million anomalies in 2023 were ransomware activity and nearly four million were APT activity.

The series should not be read as a proportional decline in risk. The 2024 PDNS ransomware disruption illustrates that a smaller number of high-impact events can carry substantial systemic consequences. Sophos reports that ransomware encryption in higher education increased from 73 to 77 percent between 2023 and 2024, recovery within one week fell from 40 to 30 percent, and mean recovery cost rose from USD 1.06 million to USD 4.02 million. The same survey identified exploited vulnerabilities as the leading technical root cause of ransomware in higher education, at 42 percent of cases. It also found that 67 percent of respondents who paid a ransom paid more than the original demand, with a median payment of USD 4.4 million. Sophos does not itemize the legacy systems that were exploited. Three categories are plausible on the basis of common practice and are offered as illustrations and not as findings. These are on premise student information systems that are costly to patch without disrupting enrollment, domain controllers and directory services whose compromise enables lateral movement, and end of support file transfer or middleware applications of the type exploited in the MOVEit campaign.

The pattern suggests that impact severity can be more informative for governance than raw incident volume. The 2024 SKKS covered 8,511 secondary-school students in 34 provinces and placed awareness mainly in the Good to Very Good IKKS range, while identifying excessive personal-data sharing and low formal incident reporting as behavioral gaps. The published SKKS methodology describes a stratified sampling design based on the Slovin formula but reports no reliability or validity coefficients for the IKKS instrument. Psychometric testing for a university population is therefore left for future research. These behavioral gaps remain relevant to a TELF. A single case of credential misuse or careless data sharing at the human layer can propagate into operationally connected and industry facing systems in a way that a purely administrative system does not permit. Because the SKKS sample was drawn from secondary schools and not from the individuals who operate these systems, its findings are best regarded as an upstream indicator and not as direct evidence about current university staff and students. The period covered by this study coincides with a lasting shift toward remote and hybrid work in higher education, which extends the network perimeter well beyond the campus. The 2023 EDUCAUSE workforce survey found that 68 percent of higher education cybersecurity and privacy staff worked at institutions offering remote or hybrid options. Faculty, staff, and students increasingly access learning platforms, student information systems, and IoT linked dashboards from home networks and personal devices that lie outside institutional patching and segmentation. This creates a distinct entry point in addition to credential phishing and vulnerability exploitation. The MOVEit campaign spread through an internet facing file transfer application. The capacity of the virtual private network, the coverage of multi factor authentication (MFA) for remote sessions, and endpoint policy for personal devices therefore require explicit treatment in the technical protection layer discussed later.

4.2. Legal Obligations and Pedagogy-Preserving Controls

Table 2 lists the duties borne by each actor in a TELF, based on the doctrinal reading of UU PDP and UU ITE and on the literature on platform governance. The matrix is a qualitative construct and does not

represent survey data. Each duty is assigned to an actor and to the process in which the duty is ordinarily exercised.

Table 2. Legal obligation matrix for TELF governance

Legal source / duty	TELF trigger/object	Governance consequence
UU PDP Arts. 34–39	High-risk processing; learner, biometric, log, assessment data	DPIA where required; safeguards; processor supervision; prevention of unlawful or unauthorized access
UU PDP Arts. 46–47	Personal-data protection failure	Written notification within 3 x 24 hours where applicable; documented accountability and incident evidence
UU ITE, Law 1/2024	Electronic systems and information	Allocate electronic-system responsibilities and preserve lawful, secure operation
Perpres 82/2022	IT/OT with potentially serious service/public impact	Infrastructure-risk benchmark; no automatic claim that a TELF is designated IIV
Partner contracts	Partner data, vendor access, hosted services	Allocate roles, confidentiality, breach cooperation, updates, and remote-access baselines

Table 2 shows that no single actor can carry the legal burden alone. The HEI holds the controller duties, yet instructors determine daily how accounts are provisioned, partners contribute their own confidentiality terms, and vendors control the patch cycle. Duties that remain unassigned at any of these points become the gaps through which a technical incident develops into a legal breach.

Table 3 pairs each threat class with the primary NIST CSF 2.0 function and with a compensating control. A compensating control reduces risk without eliminating the experimentation that justifies a learning factory. Examples include time bounded elevated privileges for reconfiguration laboratories in place of permanent administrator rights, segmented sandbox cells in place of a blanket prohibition of remote desktop access, and anonymized analytics extracts in place of raw biometric retention. A data protection impact assessment (DPIA) conducted before a new sensor is introduced applies the purpose limitation principle of UU PDP.

Table 3. Control Mapping of Threat Class, NIST CSF 2.0 Function, and Pedagogy Preserving Control

Threat Class	Primary Function	Example Compensating Control
Ransomware on instructional OT	Protect and Recover	Immutable semester image backups, rapid cell restore runbooks, offline teach pendant fallback
Insecure remote or hybrid labs	Protect and Govern	Brokered jump hosts, MFA, session recording with retention limits tied to the processing purpose
Exfiltration of learner or biometric streams	Protect and Identify	Data minimization, on device feature extraction, DPIA before new sensors
Industrial IoT or vendor supply chain compromise	Identify and Protect	Bill of materials tracking, staged update windows outside assessment peaks
Insider misuse in open labs	Govern and Detect	Named short lived credentials, logging of privileged actions, dual control for safety overrides
Integrity attacks on assessment telemetry	Protect and Detect	Signed gradebook pipelines, hash chained experiment logs, instructor attestation

Table 3 shows that most controls act on identity, data handling, or recovery, and few require the withdrawal of access from learners. The appropriate emphasis of these controls differs across the components of a TELF. Control emphasis varies by TELF domain: OT cells and remote access require strong protection and detection, learner-data services require identification and protection, and partner/vendor connections require explicit identification and governance.

These emphases are qualitative design judgments, not measured maturity scores.

4.3. Integrated Awareness and LRG-TELF Governance Model

Fig. 2 presents a four layer cybersecurity awareness framework for TELFs. Governance and policy instruments form the first layer, and technical protection controls the second. Human awareness and behavioral interventions form the third layer, and the fourth comprises the TELF components, namely learning management, student data, IoT and industrial academic interfaces, and cloud platforms. A continuous audit loop returns

findings to governance. Across the DBIR, Sophos, and BSSN data, technical controls alone were insufficient without a governance mandate and sustained awareness activity.

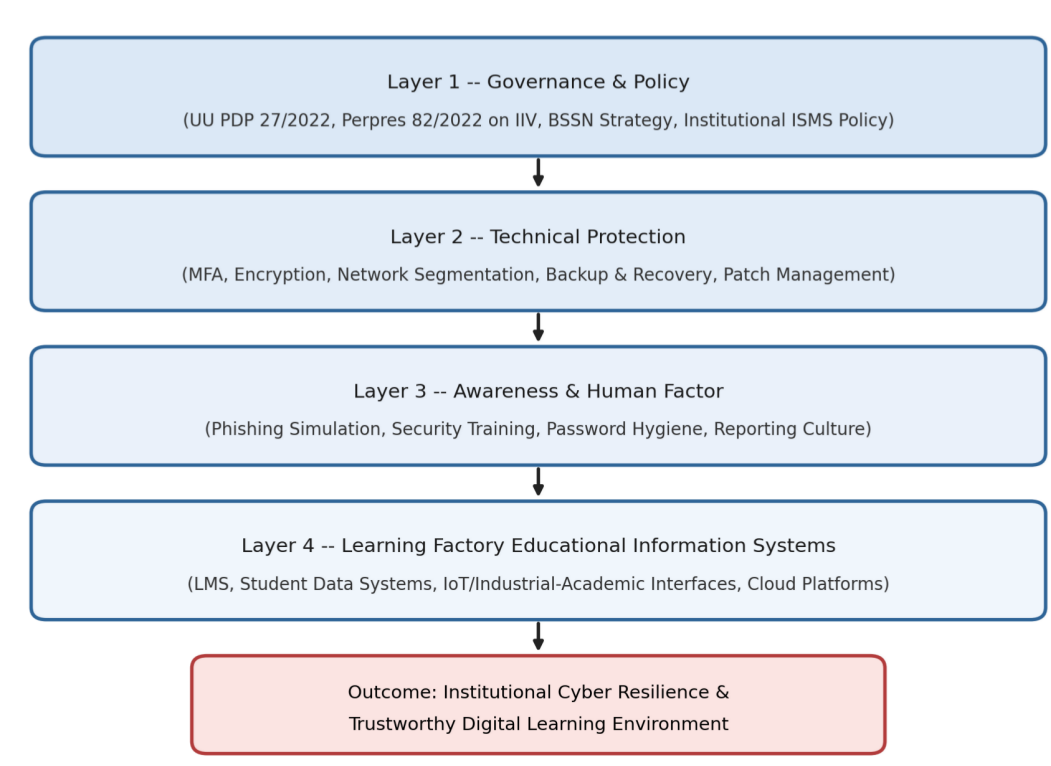


Figure 2. Proposed four layer cybersecurity awareness framework.

The layers are sequenced so that governance provides a mandate to the technical and human layers beneath it, and the audit loop returns findings from the TELF layer to governance, so that the cycle does not operate in one direction only. The second layer is specified at the level of control categories, namely MFA, encryption, network segmentation, backup and recovery, and patch management, so that it can be implemented against an established standard and not an ad hoc checklist. At the technical layer, MFA and encryption map primarily to Protect; segmentation to Protect and Detect; backup to Recover; and patch management to Identify and Protect under NIST CSF 2.0. Corresponding ISO/IEC 27001:2022 areas include access control and secure authentication, cryptography, network security, backup, and technical vulnerability management. The NIST framework is voluntary and outcome oriented and has no certification body, which makes it a low friction reference for internal planning. ISO/IEC 27001:2022 is a certifiable management system standard and is more suitable when an institution must demonstrate compliance to partners or funders. The two documents are linked through the informative references maintained by NIST, so an institution is not required to choose between them. This crosswalk is a starting reference and is not exhaustive.

LRG-TELF integrates the preceding elements into a single cycle suited to semester paced operations. Its inputs are the assets and data flows of Fig. 1, the threat classes of Table 3, and the legal obligations of Table 2. Analysis and evaluation follow ISO/IEC 27005 and NIST CSF 2.0, and each material risk is mapped to the duty that governs it. The outputs are treatment plans and accountability assignments that a dean's office, a campus CSIRT, and a partner liaison can own jointly. Statutory and contractual duties enter the model as risk acceptance criteria. A residual risk that would entail unlawful processing, an inability to notify a breach, or a breach of partner confidentiality is unacceptable irrespective of educational convenience. Openness is handled by preferring the compensating controls of Table 3 over blanket restriction, which preserves authentic access to the cell while limiting residual exposure. Fig. 3 presents the cycle.

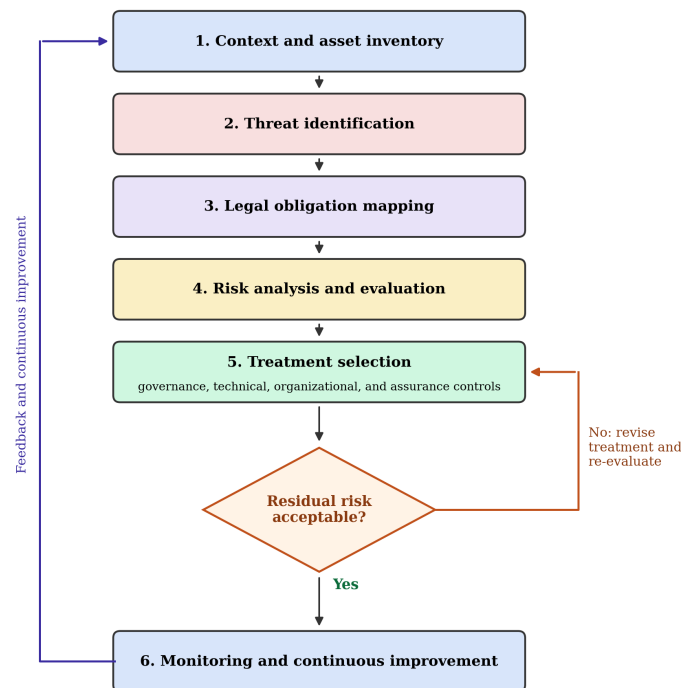


Figure 3. LRG-TELF process flow with a residual risk acceptability gate and a feedback loop.

The gate that follows treatment selection in Fig. 3 determines whether a plan proceeds to monitoring or returns for revision. The decision rule formalizes this step. It gives preference to compensating controls that preserve learning outcomes and escalates when residual risk remains above the risk appetite of the institution or when a legal criterion is not satisfied. The LRG-TELF decision rule is as follows: For each asset threat pair, map applicable legal duties, estimate risk, and select a pedagogy-preserving control. Accept only when residual risk is within institutional appetite *and* every mandatory mapped duty is satisfied; otherwise redesign the scenario, defer partner data, or refuse the processing. The decision rule is conceptual rather than implemented software. A risk below appetite is still not accepted unless every mapped legal obligation is satisfied. In operational terms, the model translates into four routines. Before each semester, the operator inventories assets and data flows against Fig. 1, supported by vulnerability management information systems. Partnership agreements allocate roles under UU PDP and UU ITE and specify breach cooperation, handling of intellectual property, and remote access baselines. Instructors follow checklists for privilege elevation and scenario sandboxing. Recovery objectives include learning continuity alongside the customary recovery time and recovery point metrics.

Curriculum designers can embed segmentation literacy and incident reporting practice into modules without converting every module into a security course. Leadership sponsorship and organizational climate determine whether these routines become established practice. LRG-TELF does not claim to be a certification pathway. It is a normative instrument for HEIs and industry operators that must reconcile open teaching with enforceable security and data protection duties. The proposals contribute to three goals. SDG 4 on quality education is supported when learning continuity and assessment integrity are protected as explicit resilience objectives. SDG 9 on industry, innovation, and infrastructure is supported by treating a TELF as resilient infrastructure with clear boundaries between OT and IT. SDG 16 on strong institutions is supported by the accountability maps and legal acceptance criteria of LRG-TELF, which make institutional duties visible and verifiable.

Several limitations qualify the findings. The four statistical sources differ in sampling frame, geographic scope, and reporting period, so comparisons across them carry more uncertainty than a single harmonized dataset would. The screening of the literature was conducted by one reviewer, which departs from a full

PRISMA protocol. The Indonesian awareness evidence derives from a secondary school sample, so its findings on over sharing and under reporting are extended to, and not measured within, a university population. None of the primary sources disaggregates data to the level of individual learning factory systems, so the discussion of IoT and OT convergence rests on the general industrial security literature and on inference and not on a dataset of learning factory incidents.

The legal analysis relies on statutes and on secondary scholarship. It does not review court decisions or regulator guidance and covers Indonesia only. The four layer framework and LRG-TELF have not been validated through expert review, a Delphi panel, or a pilot deployment, and the stated control emphases are illustrative. Both proposals should therefore be regarded as a basis for institutional discussion and not as a ready made governance instrument.

5. MANAGERIAL IMPLICATIONS

Institutional leaders should incorporate the learning factory formally into cybersecurity governance. Accountability for the governance layer in Fig. 2 should be placed at the rectorate or with the chief information officer, so that human awareness and technical controls are managed jointly and not as separate budget lines. Institutions should conduct recurring awareness training that is differentiated by role, with particular attention to phishing recognition given its role in credential based breaches. Patch management deserves priority because exploited vulnerabilities were the leading technical root cause of ransomware in higher education. Backup and recovery capability should be treated as a core resilience investment, since improved backup use in education is associated with better recovery outcomes, and budgets should account for the near fourfold increase in mean recovery cost reported by Sophos. Institutions that operate a TELF need formal cybersecurity policies and incident response procedures that refer explicitly to UU PDP, UU ITE, and Perpres 82/2022. Partnership agreements should allocate duties as outlined in Table 2, and learning continuity should be tested as a resilience indicator separate from plant uptime. Institutional leaders should also engage with regulators and university associations, which should consider whether the criteria for vital information infrastructure ought to extend to large and nationally integrated academic data systems.

6. CONCLUSION

This study examined cybersecurity exposure and legal obligations in higher education institutions that operate technology enhanced learning factories. It drew on a literature review, a doctrinal analysis of Indonesian law, and statistics from the Verizon DBIR 2024, the Sophos State of Ransomware in Education 2024 survey, and BSSN reports. The evidence indicates a high rate at which education incidents become breaches, a marked deterioration of ransomware outcomes between 2023 and 2024, and an Indonesian profile in which declining anomaly counts conceal a shift toward severe incidents affecting public and academic infrastructure.

With respect to the three research questions, the data quantify the scale and direction of the threat, and the obligation matrix identifies the duties that fall on each actor in a TELF. The four layer awareness framework and LRG-TELF provide a preliminary answer to the third question. Resilience in this setting is an institutional duty as much as a technical task, and legal requirements are most effective when they function as acceptance criteria while compensating controls preserve experimentation. The proposals are positioned against SDG 4, SDG 9, and SDG 16 and against Law 27 of 2022 and Presidential Regulation 82 of 2022.

Future research should test both proposals in Indonesian HEIs that operate learning factories. This includes longitudinal measurement of awareness among staff and students in the manner of the SKKS, reliability and validity testing of that instrument for university populations, and modeling of the relationship between awareness investment and resilience outcomes. The framework and the governance model should also be examined through an expert review or Delphi panel of chief information security officers and governance practitioners, or through a small pilot in one institution's learning factory, before wider adoption.

7. DECLARATIONS

7.1. About Authors

Imam Rahmaddani (IR)  <https://orcid.org/0000-0002-2915-2695>

7.2. Author Contributions

Validation, Conceptualization, The methodology, Formal analysis, Writing, review, and editing, Visualization was conducted by: IR, IR have reviewed and approved the final version of the manuscript.

7.3. Data Availability Statement

The corresponding author may provide the data from this study upon request.

7.4. Funding

The research, writing, and/or publishing of this work were all done without financial assistance from the authors.

7.5. Declaration of Competing Interest

The authors state that none of their known conflicting financial interests or personal connections could have had an impact on the work that was published in this publication.

REFERENCES

- [1] L. Vogt, F. Pelzer, A. Klose, V. Khaydarov, H. Lange, I. Viedt, J. Mäder, and L. Urbas, "A scalable learning factory concept for interdisciplinary engineering education: Insights from a case implementation," *Education Sciences*, vol. 15, no. 12, p. 1574, 2025.
- [2] Y. S. Fadillah, I. Yusnita, A. A. Kamal, A. Aprillia, and S. Millah, "Designing an educational information system to enhance learning factory management in higher education," *International Transactions on Education Technology*, vol. 4, no. 1, pp. 66–82, Nov. 2025.
- [3] Verizon Business, "2024 data breach investigations report," Verizon, Tech. Rep., 2024. [Online]. Available: <https://www.verizon.com/business/resources/reports/dbir/>
- [4] Sophos, "The state of ransomware in education 2024," Sophos Ltd., Tech. Rep., 2024. [Online]. Available: <https://www.sophos.com/en-us/content/state-of-ransomware>
- [5] BSSN, "Indonesia cybersecurity landscape 2023," National Cyber and Crypto Agency, Tech. Rep., 2024.
- [6] National Cyber and Crypto Agency, "Ransomware attack on temporary national data center," 2024, official Press Release.
- [7] D. Wibowo and A. Elfina, "Studi kasus serangan ransomware brain cipher pada pusat data nasional sementara indonesia," *Jurnal Mahasiswa Ilmu Komputer*, 2024.
- [8] EDUCAUSE, "2026 educause top 10: Collaborative cybersecurity," *EDUCAUSE Review*, 2025. [Online]. Available: <https://er.educause.edu/articles/2025/10/2026-educause-top-10-1-collaborative-cybersecurity>
- [9] Republic of Indonesia, "Law no. 27 of 2022 concerning personal data protection," State Gazette of the Republic of Indonesia Year 2022 Number 196, 2022.
- [10] M. Mulyati, I. Ilamsyah, A. Aris, I. Gunawan, and M. S. Zahran, "Blockchain technology: Can data security change higher education much better?" *International Journal of Cyber and IT Service Management*, vol. 1, no. 1, pp. 121–135, Apr. 2021.
- [11] S. Watini, G. Davies, and N. Andersen, "Cybersecurity in learning systems: Data protection and privacy in educational information systems and digital learning environments," *International Transactions on Education Technology*, vol. 3, no. 1, pp. 26–35, Nov. 2024.
- [12] V. Mullet, P. Sondi, and É. Ramat, "A review of cybersecurity guidelines for manufacturing factories in industry 4.0," *IEEE Access*, vol. 9, pp. 23 235–23 263, 2021.
- [13] BSSN, "National cybersecurity awareness survey 2024," National Cyber and Crypto Agency, Tech. Rep., 2024.
- [14] M. Murod, S. Anhar, D. Andayani, A. Fitriani, and G. Khanna, "Blockchain based intellectual property management enhancing security and transparency in digital entrepreneurship," *Aptisi Transactions on Technopreneurship*, vol. 7, no. 1, Mar. 2025.
- [15] R. Indrawan, A. Ratih, H. Agustian, and R. Evans, "Governance models for blockchain integrated IoT ecosystems," *Blockchain Frontier Technology*, vol. 5, no. 2, pp. 219–229, Jan. 2026.
- [16] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, and N. Meskin, "Cybersecurity for industrial control systems: A survey," *Computers & Security*, vol. 89, p. 101677, 2021.
- [17] U. H. Yulianti, Y. I. Tanjung, U. Rahardja, N. Lutfiani, and A. Valerry, "Integration of IoT and blockchain for business data security," *Blockchain Frontier Technology*, vol. 6, no. 1, pp. 62–73, May 2026.

- [18] A. Kristian, A. R. Az-Zahra, F. Hidayat, A. Y. Fauzi, and E. Kallas, "Enhancing cybersecurity risk management strategies in financial institutions: A comprehensive analysis of threats and mitigation approaches," *Journal of Computer Science and Technology Application*, vol. 1, no. 2, pp. 96–103, Aug. 2024.
- [19] U. Rahardja, P. A. Sunarya, Q. Aini, S. Millah, and S. Maulana, "Technopreneurship in healthcare: Evaluating user satisfaction and trust in AI-driven safe entry stations," *Aptisi Transactions on Technopreneurship*, vol. 6, no. 3, Sep. 2024.
- [20] R. Widayanti, A. B. Mutiara, and A. Tarigan, "Data governance in blockchain-based systems for internship grade conversion," *Aptisi Transactions on Technopreneurship*, vol. 6, no. 3, Nov. 2024.
- [21] A. Manawar, "An innovative and secure platform for leveraging the blockchain approach for online exams," *Aptisi Transactions on Technopreneurship*, vol. 5, no. 1, pp. 99–108, Mar. 2023.
- [22] Amitkumar, M. I. Sanni, and D. Apriliasari, "Blockchain technology application: Authentication system in digital education," *Aptisi Transactions on Technopreneurship*, vol. 3, no. 2, pp. 151–163, Sep. 2021.
- [23] M. Akhyar, T. M. Fadla Yoga, and E. Sukmawati, "Blockchain-based ubiquitous learning method towards higher education security," *Blockchain Frontier Technology*, vol. 1, no. 2, pp. 44–54, Jan. 2022.
- [24] Republic of Indonesia, "Law no. 1 of 2024 concerning the second amendment to law no. 11 of 2008 on electronic information and transactions," *State Gazette of the Republic of Indonesia Year 2024 Number 1*, 2024.
- [25] Indonesia Government, "Presidential regulation no. 82 of 2022 on vital information infrastructure protection," 2022.
- [26] *ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection, Guidance on managing information security risks*, ISO/IEC, Geneva, Switzerland, 2022.
- [27] *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection, Information security management systems, Requirements*, ISO/IEC, Geneva, Switzerland, 2022.
- [28] D. Alsmadi and D. Alshdaifat, "Multi-factor authentication adoption and organisational cyber resilience," *International Journal of Information Security*, 2022.
- [29] National Institute of Standards and Technology, "The nist cybersecurity framework (csf) 2.0," NIST, NIST CSWP 29, Feb. 2024.
- [30] A. N. Savitri, M. Hardini, G. Yao, and G. Yao, "Risk management model for compliance and security in blockchain powered payment platforms," *Aptisi Transactions on Management*, vol. 9, no. 2, pp. 186–196, May 2025.
- [31] F. Yusuf, R. Widayanti, S. R. Putri, and A. Wellington, "A comprehensive framework for enhancing blockchain security and privacy," *Blockchain Frontier Technology*, vol. 4, no. 2, pp. 171–182, Feb. 2025.
- [32] T. Ramayah, "Factors influencing the effectiveness of information system governance in higher education institutions (HEIs) through a partial least squares structural equation modeling (PLS-SEM) approach," *IAIC Transactions on Sustainable Digital Innovation*, vol. 5, no. 2, pp. 100–107, Apr. 2024.
- [33] H. Hamdan, U. Rahardja, M. Muhtarom, and A. Valerry, "Transforming education management with orange servant leadership and happiness practices," *Aptisi Transactions on Technopreneurship*, vol. 8, no. 2, Jun. 2026.
- [34] B. Reinheimer, L. Aldag, P. Mayer, M. Mossano, R. Düzgün, B. Lofthouse, T. von Landesberger, and M. Volkamer, "An investigation of phishing awareness and education over time: When and how to best remind users," *Computers & Security*, 2022.
- [35] A. Georgiadou, S. Mouzakitis, and D. Askounis, "Assessing MITRE ATT&CK risk using a cyber-security culture framework," *Sensors*, vol. 21, no. 9, p. 3267, 2021.
- [36] A. Prasetyo and P. W. Handayani, "Cybersecurity awareness among indonesian university students: Reliability and validity of a self-report instrument," *Journal of Information Systems*, 2022.