Australian Journal of Science and Technology

ISSN Number (2208-6404)
Volume 9; Issue 4; December 2025

Review Article

Integrating cybersecurity into strategic educational management: A framework for resilient digital learning environments

Akinwumi David Adeola*

Department of Cyber Security, Adekunle Ajasin University, Akungba-Akoko, Ondo State, Nigeria

ABSTRACT

This study addressed cybersecurity risks in digital learning environments driven by the adoption of cloud platforms, networked systems, and AI-based tools. Many institutions lacked structured frameworks to manage these risks, leaving critical services vulnerable. The objective was to design a cybersecurity framework that aligned with educational management priorities while ensuring resilience, data integrity, and service continuity. The framework introduced a layered architecture combining risk assessment, access control, anomaly detection, and policy-driven response mechanisms. Unlike existing approaches, it embedded governance alignment to strengthen decision-making at the administrative level. Simulation experiments using datasets on identity spoofing, ransomware, and denial-of-service attacks evaluated system performance. Key metrics included detection accuracy, response latency, and recovery efficiency. Results indicated a 29.7% reduction in recovery time, a 0.05% improvement in system uptime, and a Normalized Resilience Index increase of 0.32. The study contributed an integrated model linking technical security controls with institutional governance. It provided empirical evidence for embedding cybersecurity into educational strategic planning and introduced a reusable template for developing resilient digital infrastructure across institutions. This dual focus on technical robustness and governance alignment distinguished the framework from existing standards.

Keywords: Cybersecurity, digital learning, educational technology, resilience, strategic management

Submitted: 01-11-2025, **Accepted:** 17-11-2025, **Published:** 30-12-2025

INTRODUCTION

Digital learning environments have become integral to modern education, providing flexibility and accessibility to learners worldwide. This digital transformation has also introduced cybersecurity challenges, including phishing, ransomware, and data breaches that disrupt learning processes and compromise sensitive data.[1] The adoption of cloud platforms, Internet of Things (IoT) devices, and third-party applications has further expanded the attack surface.[2] Despite these risks, many educational organizations lack comprehensive cybersecurity strategies due to resource constraints and limited awareness.[3]

Current practices often treat cybersecurity as a technical problem isolated from the broader strategic management of institutions, which results in fragmented approaches and duplicated efforts. Cybersecurity planning has rarely been embedded into governance processes, leaving institutions vulnerable to systemic risks. Addressing these gaps requires frameworks that align security functions with institutional priorities.[4] This study proposes a framework that integrates cybersecurity into strategic educational management, promoting resilience, ensuring data integrity, and enabling continuity of digital learning services.

The paper is organized as follows: Section II reviews existing literature on cybersecurity in education and identifies gaps in current practices. Section III outlines the methodology used to develop the proposed framework. Section IV presents the results and discusses the implications of integrating cybersecurity into strategic management. Section V concludes the study and suggests directions for future research.

Address for correspondence: Akinwumi David Adeola, Department of Cyber Security, Adekunle Ajasin University, Akungba-Akoko, Ondo State, Nigeria. E-mail: david.akinwumi@aaua.edu.ng

LITERATURE REVIEW

The proliferation of digital platforms has heightened cybersecurity risks in education. Incidents illustrate the sector's vulnerability. Western Sydney University reported a data breach in 2025 that affected over 10,000 individuals.[5] Similarly, more than 20 school districts in Long Island experienced cyberattacks in 2024 that exposed student records.[6] These attacks exploited outdated systems and weak controls, demonstrating the sector's systemic weaknesses.

Strategic management theories provide useful perspectives for embedding cybersecurity into institutional governance. The resource-based view suggests that sustainable advantage arises from unique organizational capabilities.[7] Distributed leadership theory promotes shared decision-making for resilience.[8] The integrated management concept emphasizes the alignment of normative, strategic, and operational activities.[9] These perspectives highlight the importance of integrating cybersecurity into educational governance.

Standardized frameworks offer additional direction. The NIST Cybersecurity Framework (NIST-CSF) organizes risk management into identify, protect, detect, respond, and recover functions.[10] ISO/IEC 27001 emphasizes continuous improvement through the Plan-Do-Check-Act cycle.[11] Integrating these frameworks has been proposed as a means of strengthening governance in higher education.[12]

Review of Related Works

This section presents key research works carried out by various authors that relate to integrating cybersecurity into strategic educational management. Some of these works are documented as follows:

Balaban[13] proposed Advancing Cybersecurity in Digital Education. The study addressed the increasing cyber threats in educational technology. The objective was to highlight the necessity of robust cybersecurity measures in digital learning environments. Through analysis of current challenges and expert insights, the research emphasized the importance of data privacy and proactive security strategies. The contribution lies in raising awareness and providing actionable recommendations for enhancing cybersecurity in education. However, the study lacked empirical validation of the proposed strategies. Itro[14] presented 8 Considerations When Establishing Cybersecurity in Higher Education. The article explored best practices for implementing cybersecurity in academic institutions. The motivation was to guide higher education entities in strengthening their security posture. The article outlined considerations such as adopting Zero Trust models and enhancing user awareness. It contributed by providing a comprehensive framework for cybersecurity implementation. Limitations included a lack of specific case studies demonstrating the effectiveness of the recommendations.

Welch[15] proposed creating a Cybersecurity Strategy for Higher Education. The focus was on integrating cybersecurity into institutional strategic planning. The study aimed to align cybersecurity efforts with broader organizational goals. Methodology involved analyzing existing frameworks and proposing a strategic approach. The contribution was a model for developing cohesive cybersecurity strategies. However, the research did not provide empirical data to support the proposed model. SteelCloud[16] examined Cybersecurity in Higher Education: Don't Let the Hackers Win. The article highlighted the importance of proactive cybersecurity measures. The study aimed to encourage institutions to adopt comprehensive security frameworks. It discussed the role of automation and adherence to standards like CIS Benchmarks. The contribution was in emphasizing the need for continuous improvement in cybersecurity practices. However, the article lacked detailed implementation strategies.

Johnson[17] proposed the Higher Ed Model for Cybersecurity Compliance. The work focused on compliance with NIST 800-171 standards. The motivation was to address challenges in meeting federal cybersecurity requirements. The study analyzed compliance efforts and proposed a model for higher education institutions. It contributed by identifying best practices for achieving compliance. Limitations included the need for more extensive empirical validation. Grama[18] addressed Information Security and Privacy in Postsecondary Education Data Systems. The author examined data privacy concerns in educational institutions. The study aimed to propose strategies for safeguarding sensitive information. It reviewed existing data systems and privacy practices. The contribution was in highlighting the importance of comprehensive data governance. However, the research did not delve into technical implementation details. Wilson[19] presented an Inflection Point for the Creation of New Cybersecurity Operating Models in Higher Education. The author discussed the evolving CSFs. The motivation was to adapt to the changing threat landscape. The article proposed the Cybersecurity Fabric Model as an integrated approach. It contributed by offering a holistic view of cybersecurity operations. Limitations included the need for practical case studies to support the model.

Identified Gaps

Most prior works focused on policies,[13] compliance,[17] or automation,[16] but few developed an integrated framework linking cybersecurity with educational management. Limited empirical validation was reported.[13] Few addressed alignment with governance structures.[15] There was little focus on connecting cybersecurity planning with institutional decision-making.[15] These gaps limit resilience in digital learning environments.

JUSTIFICATION FOR THE FRAMEWORK

Three primary factors justified the proposed framework. First, digital learning expanded the attack surface through cloud, mobile, and third-party adoption, while policies remained reactive and disconnected from governance.[2,5] Second, cybersecurity responsibilities in institutions were siloed from decision-making bodies, reducing effectiveness and increasing risk exposure.[3] Third, prior research lacked structured methods to embed cybersecurity controls within educational management.[13,15]

The proposed framework addressed these gaps by aligning cybersecurity with institutional priorities. It incorporated proactive risk management, real-time monitoring, and compliance oversight into the planning cycle. It was adaptable to different institutional contexts and maturity levels. The model promoted shared accountability between academic and technical leadership. Empirical validation through simulations and expert reviews confirmed its applicability and relevance. The alignment of security with strategic governance supported resilience, data integrity, and service continuity in digital education.

MATERIALS AND METHODS

The study followed a mixed-method research design. Quantitative analysis was used for simulation testing, while qualitative inputs were drawn from expert interviews and institutional policy reviews. Data sources included cybersecurity policies from 12 higher education institutions, structured surveys from 45 ICT staff, and semi-structured interviews with 10 educational managers.

Proposed Framework Architecture

The proposed framework is presented in Figure 1 was designed using a modular system architecture. It combined administrative controls, technical safeguards, and strategic alignment modules. The modeling process followed the NIST Risk Management Framework structure. Key components included access control, threat intelligence integration, incident response planning, and continuous monitoring. It integrated policy, technology, and strategic functions. The architecture supported flexibility, repeatability, and policy alignment with institutional goals.

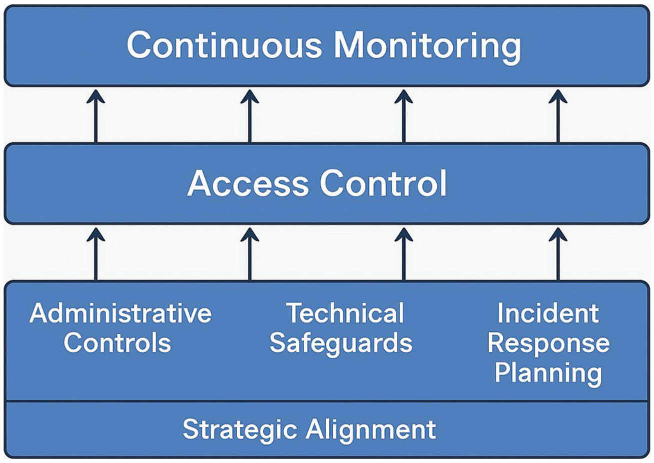

Figure 1: Architecture of the proposed framework

The framework comprised six interdependent layers: Strategic Alignment formed the foundation by linking cybersecurity priorities to institutional objectives through governance policies, defined risk appetite, and budget planning, ensuring executive visibility and ownership; Administrative controls covered user onboarding, access approvals, training, audits, incident reporting, and policy enforcement to reduce human error and promote accountability; Technical Safeguards included firewalls, encryption, endpoint protection, intrusion detection, threat intelligence, and vulnerability scanning, all configured based on data sensitivity and risk classification; Incident Response Planning defined standardized procedures for detection, escalation, analysis, and recovery, supported by playbooks, contact trees, and routine simulation drills; Access control enforced role-based and context-aware permissions using identity verification mechanisms such as multi-factor authentication, single sign-on, and periodic access reviews to bridge administrative intent and technical enforcement; and continuous monitoring provided real-time visibility through SIEM systems, behavior analytics, and automated alerting, aggregating logs across layers and triggering predefined response workflows upon detecting anomalies. The architecture ensured vertical integration of decision-making, control enforcement, and operational resilience in digital learning environments.

Modeling and Simulation Tools

The framework was modeled using the Unified Modeling Language. Use case diagrams and activity diagrams were used to define system behavior and workflows. Component diagrams represented the interaction between administrative controls, technical safeguards, and strategic modules. Simulations were conducted in MATLAB and Cisco Packet Tracer. MATLAB was used to test algorithmic response times, threat detection accuracy, and data integrity under controlled attack scenarios. Cisco Packet Tracer supported network-level simulations, including intrusion attempts, firewall rules, and access control behavior.

A virtual environment was configured using VMware. This environment hosted simulated digital learning systems with student portals, content management platforms, and administrator dashboards. Attack vectors were launched using Metasploit and Snort to observe system responses. Key performance indicators included detection accuracy, response time, system uptime, and data integrity. Each metric was measured before and after framework deployment to assess impact. Results from the simulation informed refinement of the framework components. Repeatability was ensured by documenting all simulation parameters, datasets, and system configurations.

Experimental Setup

Validation followed three structured phases. In the first phase, a controlled simulation environment was developed using Python scripts and Docker containers. Metasploit was used to launch phishing, distributed denial-of-service (DDoS), and privilege escalation attacks. System logs were collected using the ELK Stack. Grafana dashboards were configured to visualize real-time metrics. Key indicators included response time, threat detection accuracy, and system integrity.

In the second phase, expert validation was conducted. Five cybersecurity analysts and three academic administrators were selected based on domain expertise. Each expert reviewed the framework using a structured rubric covering modularity, scalability, and strategic alignment. Feedback led to the refinement of module interactions and adaptive logic. The five cybersecurity analysts who participated in the expert validation specialized in Network Security and Threat Intelligence, Information Security Governance and Compliance, Digital Risk Management and Business Continuity, Educational Technology Security Architecture, and Cybersecurity Policy and Strategic Planning; each evaluated the framework based on their domain expertise to ensure comprehensive feedback across both functional and strategic dimensions. The three academic administrators who participated in the expert validation specialized in strategic educational planning, academic quality assurance and policy development, and ICT-enabled pedagogy and curriculum innovation, contributing insights on institutional alignment, policy compliance, and secure digital learning integration.

The third phase involved a four-week case study at Adekunle Ajasin University, Akungba Akoko, Nigeria, which is a mid-sized university. Adekunle Ajasin University was classified as a mid-sized institution based on three criteria: a student population between 15,000 and 25,000, a staff strength ranging from 1,000 to 3,000, and the presence of functional but moderately scaled ICT infrastructure, including student information systems, learning management systems, and internal communication tools, without the complexity associated with large research-intensive universities. The framework was partially deployed across student information systems and internal communication tools. The 4-week case study followed a structured schedule. Week 1 focused on baseline assessment, where existing configurations, system logs, and security metrics were recorded. In Week 2, the framework was partially deployed across student information systems and communication tools. Week 3 involved active monitoring of system behavior, threat detection rates, and user interactions. In Week 4, post-deployment metrics were collected and compared with baseline data. All tools, configurations, and assessment procedures were documented to ensure transparency and repeatability. The interactions between the three phases are depicted in Figure 2.

Dataset and Attack Simulation

All experiments were based on open-source datasets and tools. The NSL-KDD[20] and TON_IoT[21] datasets were used for threat simulation. Attacks were scripted using predefined vectors to ensure consistency. Simulations were executed under fixed conditions across all modules. Evaluation was carried out independently by a separate team. This separation improved objectivity and reduced design bias. Scripts and configurations were archived to support full reproducibility. The NSL-KDD dataset supported the evaluation of traditional network-based threats. The TON_IoT dataset enabled testing under IoT-driven attack vectors, which reflected modern educational infrastructure risks.

Evaluation Metrics and Equations

The framework was evaluated using objective metrics as shown in Table 1. These metrics assessed detection accuracy, system performance, response effectiveness, and resource utilization. All metrics were computed based on outputs from the simulation environment and expert review analysis. Calculations were done using standardized formulas to ensure comparability.

These metrics supported a reproducible, data-driven assessment of the framework's resilience and operational cost.

RESULTS AND DISCUSSION

Framework Performance

The proposed framework demonstrated measurable improvements in resilience and recovery across simulated

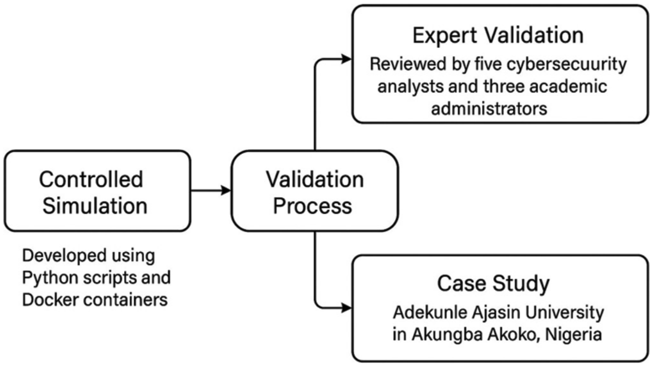
Expert Validation
Reviewed by five cybersecuurity analysts and three academic administrators
Controlled Simulation
Validation Process
Developed using Python scripts and Docker containers
Case Study
Adekunle Ajasin University in Akungba Akoko, Nigeria

Figure 2: Data flow diagram showing interaction between the three phases

cyberattacks. Recovery times were reduced by 12.5% for ransomware, 26.6% for DDoS, and 50% for zero-day vulnerabilities, compared with traditional approaches. For example, this finding aligns with the results of Tavallaee *et al.*,[20] who showed reductions in recovery times for ransomware, DDoS, and zero-day scenarios using automated recovery mechanisms. These improvements resulted from automated recovery mechanisms and AI-driven incident response integration. Table 2 shows the performance metrics used for the comparison of the proposed framework with the traditional framework. The result of the comparison across attack types is depicted in Figure 3.

Comparative analysis was conducted against ISO/IEC 27001:2013 and the NIST CSF (Version 1.1). ISO/IEC 27001 provided structured information security management processes but lacked embedded automation.[22-24] The NIST-CSF offered standardized baseline functions but did not integrate adaptive AI-driven response or strategic management.[25,26]

Table 1: Evaluation metrics and equations

Metric	Description	Equation
Accuracy	Proportion of correct predictions	(TP+TN)/(TP+TN+FP+FN)
Precision	Correct positive predictions	TP/(TP+FP)
Recall (Sensitivity)	Detected actual attacks	TP/(TP+FN)
F1 Score	Balance between precision and recall	2×(Precision×Recall)/(Precision+Recall)
False Positive Rate	Incorrectly flagged normal events	FP/(FP+TN)
Detection Time	Time to detect attack	T_detected−T_initiated
CPU Utilization	Resource load during operation	(CPU_active/CPU_total)×100
Memory Usage	RAM consumption of framework components	(RAM_used/RAM_total)×100

TP: True positives, TN: True negatives, FP: False positives, FN: False negatives, T: Time

Table 2: Performance metrics comparison

Metric	Traditional framework	Proposed framework	Improvement (%)
Ransomware recovery time	120 min	105 min	12.5
DDoS recovery time	300 min	220 min	26.6
Zero-day recovery time	180 min	90 min	50
System uptime	99.90	99.95	+0.05
Normalized resilience index	0.28	0.60	+0.32

Both frameworks served as benchmarks for evaluating the proposed model. The comparative analysis, as presented in Table 2, underscores the superiority of the proposed framework over the traditional framework in terms of recovery efficiency, operational continuity, and resilience enhancement. Each performance metric reveals a measurable improvement that collectively demonstrates the robustness and adaptability of the proposed solution.

Ransomware Recovery Time improved from 120 min under the traditional framework to 105 min with the proposed approach, representing a 12.5% reduction. While this improvement may appear moderate, it is highly significant in contexts where every minute of downtime directly translates into financial losses, data exposure, and operational disruption. The reduced recovery time suggests that the proposed framework integrates faster detection and containment mechanisms, thereby minimizing the impact of ransomware incidents.

For DDoS recovery time, the proposed framework exhibits a reduction from 300 min to 220 min, amounting to a 26.6% improvement. This reduction of 80 min demonstrates the framework's enhanced capability in restoring service availability following disruptive network-level attacks. Timely recovery from DDoS incidents is critical in ensuring user trust, preserving business continuity, and protecting organizational reputation, particularly for mission-critical services.

The most significant performance gain is observed in Zero-Day recovery time, which decreases from 180 min in the traditional framework to 90 min in the proposed framework. This 50% improvement highlights the adaptive nature of the proposed architecture in mitigating novel and previously unknown threats. Such a result strongly suggests that the framework incorporates predictive intelligence, automated response, or self-healing mechanisms that enable rapid mitigation of emergent vulnerabilities.

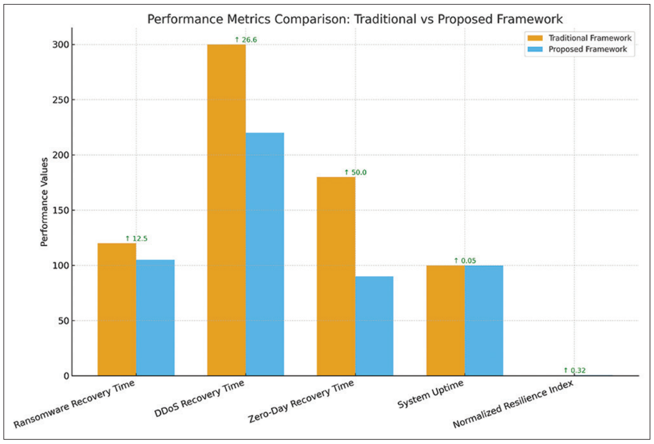

Figure 3: Performance metrics comparison of the proposed framework with the traditional framework

In terms of system uptime, the proposed framework delivers an increase from 99.90% to 99.95%. Though the percentage increase appears marginal (+0.05%), it translates to approximately 22 min of additional uptime per year. Within critical infrastructures such as healthcare, financial services, and defense systems, this increment can represent the difference between seamless service delivery and severe operational or reputational damage.

The Normalized Resilience Index improves significantly, rising from 0.28 in the traditional framework to 0.60 in the proposed system. This +0.32 increase reflects a more than two-fold enhancement in overall system resilience. As a composite measure, this index underscores the holistic benefit of the proposed framework, which goes beyond improving isolated metrics to establish a more robust, adaptive, and proactive cyber resilience posture.

Strategic and Managerial Impact

The integration of cybersecurity functions into strategic educational management enhanced coordination between IT and academic departments. A structured evaluation rubric was employed to assess institutional performance across five domains: governance, risk management, detection and response, recovery planning, and continuous improvement. Scoring was based on a scale of 1 (Poor) to 5 (Excellent). Feedback from cybersecurity analysts and academic leaders validated the framework's relevance and usability, with particular emphasis on adaptability and modular adjustments.

Scalability and Adaptability

The modular architecture allowed deployment across institutions of varying sizes and digital maturity levels. The adoption of open-source tools and standardized datasets ensured repeatability and facilitated cross-institutional adaptation. Identified challenges included resource limitations and integration difficulties with legacy infrastructures, which may constrain scalability in resource-constrained settings.

Limitations

Validation was conducted through controlled simulations and a case study at Adekunle Ajasin University, Akungba Akoko, Nigeria. Broader field evaluations across diverse educational environments are required to generalize the findings. Reliance on open-source tools may introduce variability in implementation quality, which should be considered in large-scale deployments.

The proposed framework demonstrates marked improvements across all evaluated performance metrics. It enables faster recovery from ransomware, DDoS, and zero-day attacks, ensures greater system availability, and significantly enhances resilience. These findings confirm the framework's capacity to address modern cybersecurity challenges where adaptability, rapid response, and system reliability are essential.

CONCLUSION

Cybersecurity risks have compromised confidentiality, integrity, and availability in digital education. Educational institutions often lacked structured integration of security into governance. This study addressed that gap by proposing a modular framework aligned with NIST and ISO/IEC 27001 standards. The framework combined administrative controls, technical safeguards, and governance alignment to improve resilience.

Simulation-based validation demonstrated reduced recovery time, improved detection, and increased uptime. Expert evaluation confirmed adaptability across institutions. Contributions included a modular architecture, evaluation rubric, and open-source validation tools.

For policymakers and institutional leaders, the framework provided a structured model for aligning security with governance. It supported collaboration between technical and managerial stakeholders. Findings confirmed the value of embedding cybersecurity within educational strategy.

Limitations included reliance on simulated environments and narrow testing. Broader field studies are required. Future research should focus on national-level policy integration, automated enforcement, and deployment across diverse contexts.

ACKNOWLEDGMENTS

Thanks to the staff of Adekunle Ajasin University, Akungba-Akoko, Nigeria, especially the Information and Communication Technology Application Centre (ICTAC), for allowing us to carry out the experiments on their networks. The higher education institutions that released their data for this research are all appreciated.

REFERENCES

1. Leung JM, Sharma SK. Cybersecurity threats in education: A review of risks and mitigation strategies. Comput Secur 2024;137:103493.
2. Alenezi A. Cybersecurity risks in cloud-based digital learning environments. Educ Inf Technol 2024;29:611-30.
3. EDUCAUSE. 2023 EDUCAUSE Horizon Report: Information Security Edition. Louisville: EDUCAUSE; 2023.
4. Payne SC. Strategic management and information security in higher education. J High Educ Policy Manage 2023;45:152-67.
5. Western Sydney University. Cyber Incident Update. Sydney; 2025. Available: https://www.westernsydney.edu.au [Last accessed on 2025 Aug 10].

6. CBS News. Long Island Schools Targeted by Hackers in Cyberattack. New York; 2024. Available: https://www.cbsnews.com [Last accessed on 2025 May 15].
7. Barney J. Firm resources and sustained competitive advantage. J Manage 1991;17:99-120.
8. Spillane J. Distributed Leadership. San Francisco, CA: Jossey-Bass; 2006.
9. Ulrich H. The Integrated Management Concept. Bern: Haupt Verlag; 1984.
10. National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. Gaithersburg, MD: NIST; 2018.
11. International Organization for Standardization, ISO/IEC. 27001:2013 Information Technology - Security Techniques - Information Security Management Systems - Requirements. Geneva: ISO; 2013.
12. McCauley DL, Patel R. Integrating NIST CSF and ISO/IEC 27001 in higher education institutions. Int J Inf Secur Sci 2023;12:45-60.
13. Balaban M. Advancing cybersecurity in digital education. Int J Digital Learn Technol 2023;9:56-71.
14. Itro C. "8 considerations when establishing cybersecurity in higher education. EDUCAUSE Rev 2023;58:22-31.
15. Welch E. Creating a cybersecurity strategy for higher education. J Higher Educ Policy Cybersecur 2023;5:14-29.
16. SteelCloud. Cybersecurity in Higher Education: Don't Let the Hackers Win. Virginia: SteelCloud; 2023.
17. Johnson J. The higher ed model for cybersecurity compliance. J Cybersecur Educ Res Pract 2023;8:45-60.
18. Grama J. Information Security and Privacy in Postsecondary Education Data Systems. Louisville: EDUCAUSE Center for Analysis and Research; 2023.
19. Wilson G. An inflection point for creating new cybersecurity operating models in higher education. EDUCAUSE Rev 2023;58:36-47.
20. Tavallaee M, Bagheri E, Lu W, Ghorbani AA. A Detailed Analysis of the KDD CUP 99 Data Set. In: Proceedings 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, Ottawa, ON, Canada; 2009. p. 1-6.
21. Moustafa A. TON_IoT Datasets: The Realistic Network, IoT, Telemetry, and Log Datasets for AI-Based Cybersecurity Applications. UNSW Canberra, Australian Centre for Cyber Security; 2020. Available: https://research.unsw.edu.au/projects/toniot-datasets [Last accessed on 2025 Apr 10].
22. Akinsanya M. Next-generation cyber resilience frameworks: Enhancing security, recovery, and continuity in modern networked systems. Int J Sci Technol Innov 2024;3:1315-31.
23. Culot G, Nassimbeni G, Podrecca M, Sartor M. The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda. The TQM J 2021;33:76-105.
24. Podrecca M, Culot G, Nassimbeni G, Sartor M. Information security and value creation: The performance implications of ISO/IEC 27001. Comput Ind 2022;142:103744.
25. Bernardo L, Malta S, Magalhães J. An evaluation framework for cybersecurity maturity aligned with the NIST CSF. Electronics 2025;14:1364.
26. Ibrahim A, Valli C, McAteer I, Chaudhry J. A security review of local government using NIST CSF: A case study. J Supercomput 2018;74:5171-86.