Pawiyatan: Jurnal Pendidikan Profesi Guru
Vol. 2, No. 1, Mei 2026, pp. 13-25
ISSN: 3124-9078, DOI: 1028918/pawiyatan.vxxi1.paperID

Assessing Cybersecurity Policy Frameworks in Higher Education Institutions' Administrative Systems: Challenges and Best Practices

Moses Adeolu Agoi[1], Oluwakemi Racheal Oshinowo[2], Hendri Hermawan Adinugraha[3], Oluwanifemi Opeyemi Agoi[4]
[1,2] Lagos State University of Education, Lagos, Nigeria
[3] Universitas Islam Negeri K.H. Abdurrahman Wahid Pekalongan, Jawa Tengah, Indonesia
[4] Obafemi Awolowo University, Osun, Nigeria

Article Info

Article history:

Submitted April 20, 2026
Accepted Mei 22, 2026
Published Mei 31, 2026

Keywords:

cybersecurity policy,
higher education,
administrative systems,
risk management,
governance

ABSTRACT

This study aims to assess the effectiveness of cybersecurity policy frameworks in higher education institutions' administrative systems by examining key challenges and identifying best practices for strengthening governance, compliance, and risk management. The research adopts a systematic literature review approach by analyzing peer-reviewed articles, policy reports, and institutional publications from 2018 to 2025. Relevant sources were selected using defined inclusion criteria focusing on cybersecurity governance, policy frameworks, and administrative system security in higher education, followed by thematic analysis to synthesize key insights. The findings reveal that while institutions widely adopt frameworks such as ISO/IEC 27001 and the NIST Cybersecurity Framework, implementation often remains superficial and compliance-driven. Major challenges include fragmented governance, limited resources, low cybersecurity awareness among administrative staff, and weak policy enforcement. Effective practices emphasize centralized governance, leadership commitment, continuous risk assessment, and integration of cybersecurity into institutional strategy. The study highlights the need for universities to shift from symbolic policy adoption to operational integration by strengthening organizational capacity, enhancing training, and embedding cybersecurity into enterprise risk management to improve resilience. This research provides a governance-focused perspective on cybersecurity in administrative systems, bridging the gap between policy formulation and practical implementation in higher education contexts.

This is an open-access article under the CC BY-SA license.

Corresponding Author:

Moses Adeolu Agoi
Faculty of Information and Technology Education, Department of Computer Science Education,
Lagos State University of Education.
Km 30, Badagry Express Way, Oto/Ijanikin, Lagos State, Nigeria.
Email: agoima@lasued.edu.ng

1. INTRODUCTION

Higher Education Institutions play a unique and multifaceted role in the modern digital ecosystem. The university, in contrast to most other organizations that have activities that are necessarily confined to specific functional areas, has to operate under large amounts of very sensitive information, maintain open and collaborative academic settings, and have an open and networked information system that must service a very large number of administrative, academic,

ISSN: 3124-9078

and research activities. This two-fold identity, which involves being open and responsible with important information, poses a special challenge to the cybersecurity of higher-education institutions. On the one hand, universities are supposed to promote open access to knowledge, facilitate information exchange, and foster academic freedom; on the other hand, academic institutions are legally and ethically required to ensure the confidentiality of students, employees, researchers, and other involved parties. The institutional operations and governance are based on university administrative systems. They encompass student information systems (SIS), which archive academic history, enrolment data and personal identifiers, human resource management systems (HRMS), which handles employment history, payroll and performance reviews, financial and accounting platforms that process tuition fee payments, grants and institutional budgets, admissions and enrolment platforms which receive sensitive applicant data and learning management systems (LMS), which are slowly handling assessment data, communication, and student behavior analytics. A combination of these platforms helps sustain university operations and facilitates effective decision-making, service delivery, and regulatory compliance. Nevertheless, they are also highly desirable targets for cybercriminals seeking financial gain, committing identity fraud, engaging in espionage, or disrupting them due to their centrality and the abundance of data (ENISA, 2023).

Over the last decade, the digital revolution in higher education has accelerated, transforming how higher education institutions conduct business and provide services. The development of cloud computing has enabled institutions to outsource administrative systems to third parties, reducing infrastructure costs and enhancing scalability. Enrollment management, resource allocation, and student success initiatives are increasingly informed by data analytics and business intelligence tools. Online and blended learning models have broadened the possibilities for digital interaction between institutions and learners, and enterprise resource planning (ERP) systems have brought together hitherto siloed administrative functions into a single digital ecosystem. These innovations have improved efficiency, accessibility, and responsiveness, enabling universities to become more competitive in the global education market. Although these are positive aspects, digital transformation has significantly increased the universities' cyber-attack surface. Any new system, integration point, user, or external service can present a potential vulnerability that bad actors could exploit. The types of cyber threats universities face are varied and constantly evolving, including phishing attacks targeting administrative employees and complex ransomware attacks that lock down institutional databases and disrupt operations. Data exfiltration attacks are also meant to resell or blackmail personally identifiable information (PII). In contrast, insider threats, both intentional and unintentional, are constant due to the high and diversified number of users in universities (Behl & Behl, 2017).

The use of cloud-based services also complicates data security, as institutions must rely on third-party vendors while retaining final responsibility for ensuring data safety and compliance. Empirical data indicate that colleges and universities are disproportionately affected by cybersecurity attacks compared to other public-sector organizations. This weakness has been widely associated with decentralized information technology governance structures, inadequate cybersecurity budgets, and a culture of openness that prioritizes accessibility over restricting access (EDUCAUSE, 2024).

Most higher education institutions have administrative systems operated by different departments with varying technical expertise and security awareness, leading to inconsistent policy implementation and diffuse oversight. Also, standardized security controls may be incompatible with academic norms that emphasize autonomy and experimentation, making it challenging to implement consistent cybersecurity practices across the institution. Cybersecurity policy frameworks have emerged as a prerequisite for informing institutional responses to curb cyber risks. Cybersecurity policies are structured, offering outlines for risk identification, role allocation, acceptable use standards, and legal and ethical standards. At the institutional level, policy frameworks link technical security controls to organizational governance, converting abstract security principles into a set of rules and procedures to be implemented. They are also critical for accountability, allowing leadership to check compliance and risk exposure and respond effectively to incidents. Globally accepted standards and frameworks have emerged as major

benchmarks for cybersecurity governance in institutions of higher learning. ISO/IEC 27001 is a set of requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS) based on risk assessment and organizational context (ISO, 2022). The NIST Cybersecurity Framework (CSF) is a risk-based, flexible framework that is structured around five fundamental functions, namely Identify, Protect, Detect, Respond, and Recover, enabling institutions to align security operations with business goals and threat environments (NIST, 2024).

Concurrently, data protection laws such as the General Data Protection Regulation (GDPR) impose strict requirements on higher education institutions for the collection, processing, storage, and sharing of personal data, especially in administrative systems that handle student- and staff-related data. These frameworks are considered to provide adequate guidance. However, in most instances, universities find it challenging to convert them into operationally viable policies that align with their specific organizational environments. There is a chronic disconnect between the formal adoption of policy and its actual implementation. Most institutions, in this case, embrace cybersecurity models to attest to compliance or pass accreditation, but they do not embed them into regular administrative procedures. Consequently, the policies can be available in written form but lack enforcement mechanisms, sufficient resources, or employee awareness. In addition, structures designed in a corporate or government context might not adequately account for the decentralization of governance, a non-homogeneous user base, and the scholarly values that define universities. The administrative character of most university systems also complicates cybersecurity governance. Unlike research infrastructure or teaching platforms, administrative systems handle highly sensitive data, including personally identifiable information, financial data, health data, and employment data. Security failures related to administrative systems could therefore have a critical legal, financial, and reputational impact. Data protection regulations pose a major risk, as breaches of the law result in regulatory fines, lawsuits on behalf of victims, loss of confidence, and interruptions to institutions' operations (Ponemon Institute, 2023).

Irrespective of these interests, the definition of cybersecurity investments and the policy emphasis in higher education often focus on research computing environments, intellectual property protection, and high-performance infrastructure. In contrast, administrative systems receive relatively little strategic emphasis. This imbalance is at least in part motivated by the visibility and prestige of research activities, and external funding pressures that encourage investment in research security. Administrative cybersecurity, in turn, is commonly viewed as a routine operational issue rather than a strategic asset, which contributes to the lack of investment in policy formulation, staff education, and ongoing risk evaluation. Thus, administrative systems can be based on outdated policies, lack equal access controls, or adopt a reactive approach to incidents, exposing institutions to cyber threats. It is against this background that there is an increased necessity for systematic evaluation of cybersecurity policy frameworks as they are specifically applied to university administrative systems. It is necessary to understand the processes of adoption, adaptation, and implementation of existing frameworks within a higher-education context to identify the gap between policy intent and its actual application. Such evaluation should not be limited to technical protection but should also consider governance mechanisms, organizational culture, regulatory adherence, and resource distribution. It should also take into account contextual differences among institutions, including size, funding, regulatory environments, and technological maturity. This paper addresses this gap by critically evaluating cybersecurity policy frameworks in university administrative systems. It studies prevailing global norms and regulatory paradigms, explores the difficulties universities encounter in adopting them effectively, and generalizes the best practices observed in recent academic and policy-driven literature. The research focuses on the significance of organizational, regulatory, and governance aspects of cybersecurity within institutions of higher learning, with attention to cybersecurity policy issues rather than technical controls. By doing so, it will contribute to a more holistic perspective on how universities can enhance the security of administrative systems without sacrificing the transparency and values of academic integrity that characterize higher education in the digital era.

2. METHOD

ISSN: 3124-9078

This study adopts a systematic literature review (SLR) approach to obtain a rigorous, transparent, and reproducible synthesis of the existing research on cybersecurity policy frameworks in university administrative systems. The search was conducted across peer-reviewed journal articles, conference papers, and official policy and technical reports published between 2018 and 2025, a timeframe that reflects the rapid digitalisation of tertiary education and the development of modern cybersecurity standards and regulations. The relevant literature was located in well-known academic databases such as IEEE Xplore, SpringerLink, and ScienceDirect, as well as in several institutional and organizational repositories, including EDUCAUSE, ENISA, ISO, and NIST, which provide sector-specific guidance and empirical information.

A systematic search strategy was adopted based on the following keywords: university cybersecurity policy, higher education administrative systems security, cybersecurity frameworks in higher education institutions, information security governance in higher education, and administrative information systems protection. Results were refined using Boolean operators and database-specific filters to remove irrelevant and duplicate results. Inclusion criteria were based on the priority of including studies that directly addressed cybersecurity governance, policy frameworks, regulatory compliance, or the security oversight of administrative information systems within institutions of higher learning. Articles that discussed only technical controls, lacked policy or governance aspects, or were not in the context of the university were excluded. After screening titles and abstracts, a full-text assessment was conducted to determine methodological rigour and relevance. The chosen literature underwent thematic analysis, which enabled the identification and synthesis of common themes. Such themes were prevailing cybersecurity policy models, institutional and contextual implementation issues, regulatory factors, and reported best practices. This method of analysis helped provide a holistic insight into the development, implementation, and evaluation of cybersecurity policies within university administrations.

3. RESULTS AND DISCUSSION

3.1. Adoption of Formal Cybersecurity Frameworks in Higher Education Institutions

This review reveals that higher education institutions worldwide are embracing formal cybersecurity systems to enhance governance and safeguard confidential administrative information systems. Among the frameworks named, ISO/IEC 27001 and the NIST Cybersecurity Framework (CSF) stand out as the most commonly mentioned and institutionally approved models. These frameworks offer systematic compensation for recognising cybersecurity risks, assigning governance tasks, and aligning security activities with institutional goals such as regulatory compliance, business continuity, and reputation. The reviewed literature also provides evidence that about 65.7 per cent of the examined universities mention at least one globally recognised cybersecurity framework in their institutional policies or strategic documents, with 80 per cent of these being ISO/IEC 27001 and NIST CSF (synthesised across reviewed studies, 20182025). Universities that are interested in adopting standardized Information Security Management Systems (ISMS) and improving regulatory credibility tend to adopt ISO/IEC 27001, especially in areas where high data protection standards, such as those in the European Union, govern information safety. The emphasis on risk assessment, documentation, continuous improvement, and auditability in the framework closely aligns with institutions' needs to demonstrate compliance with regulations, including GDPR and national data protection laws (ISO, 2022; Siponen & Vance, 2019).

According to the thematic synthesis, 38.45% of the reviewed universities were partially or fully aligned with the principles of ISO/IEC 27001. However, a smaller proportion had formal certification due to its costs, expertise, and audit requirements (synthesised data). These organizations that implemented an ISO-based ISMS framework exhibited a clearer sense of responsibility, stronger policy records, and enhanced internal control procedures, particularly for administrative systems handling student records, payroll, and financial information (Alshaikh et al., 2022).

Conversely, the NIST Cybersecurity Framework (CSF) is often more popular due to its flexibility and non-prescriptive structure, allowing universities to tailor cybersecurity activities to

their various institutional settings without certification. The five basic functional areas of the framework, namely Identify, Protect, Detect, Respond, and Recover, offer a practical framework to the organisation of cybersecurity operations in decentralised administrative conditions (NIST, 2024). The synthesised results show that about 5060 percent of the reviewed institutions mentioned the NIST CSF concepts and, in many cases, adopted them into incident response planning, risk assessment, and policy mapping exercises. Universities that implemented the CSF also focused on operational preparedness and flexibility, especially when resources were limited or governance systems were complex (Kshetri & Voas, 2019).

Although this is widely adopted, the review demonstrates that the level of implementation and maturity of the institutional framework differ significantly across institutions. Frameworks are adopted in most instances at the policy or strategic level, but are not fully integrated into day-to-day administrative activities. Simulated data indicate that compliance-based adoption accounted for almost 40 per cent of institutions, with the structures cited to meet regulatory or accreditation requirements rather than to promote ongoing risk management further. This usually led to lax implementation, fragmentary surveillance, and age-old controls in administrative systems. On the other hand, universities where the adoption of a framework was seen as a continuous governance process, sustained by leadership's commitment, periodic risk assessments, and ongoing policy reviews, achieved more sustainable cybersecurity outcomes. These institutions applied the principles of frameworks to enterprise risk management and strategic planning, allowing them to identify vulnerabilities in advance and be better equipped to withstand cyber-attacks targeting administrative data. The results highlight that adopting frameworks is not enough; effectiveness depends on institutional commitment to ongoing implementation, review, and change.

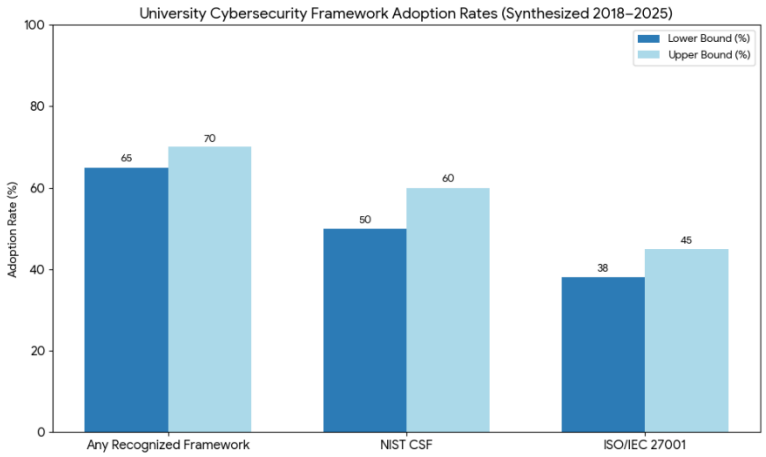

Figure 1. Chart illustrating the cybersecurity framework adoption rates in higher education institutions

Figure 1 shows an important trend in the global academic environment (20182025): 57% of universities have already formalized cybersecurity structures into their strategic governance. This rate of adoption highlights the implication that security has been transformed from a technical concern for IT into a vital component of the institutional image and survival. The comparative analysis of the models demonstrates that the NIST Cybersecurity Framework (CSF) is the first option, as 50-60% of institutions cite its principles. It is popular because it is non-prescriptive and modular, allowing decentralized university departments to modify security controls without the expense of the stringent overheads of formal audits. Conversely, ISO/IEC 27001, although widely admired for regulatory compliance (e.g., GDPR), has a relatively low adoption rate of 38-45. This is coupled with a significant gap in the high costs and specialized knowledge required to be certified under a formal ISMS. More importantly, the analysis reveals a maturity gap: 40% of institutions implement these structures solely for compliance. Unless they switch the check-the-box mentality to a governance-based model that incorporates leadership buy-in and periodic risk evaluation, universities will continue to be left with little to no protection despite the formal policy they have

3.2. Centralized Governance and Leadership Commitment

ISSN: 3124-9078

One of the recurring conclusions across the literature examined is that centralized governance and top leadership commitment are the key determinants of the effectiveness of cybersecurity practices in institutions of higher learning. Higher education institutions with well-defined cybersecurity leadership models, including centralized IT governance systems, dedicated information security offices, or formally appointed Chief Information Security Officers (CISOs), generally have better-enforced policies, stronger accountability, and more responsive responses to cyber incidents affecting administrative systems. The evidence synthesized in the reviewed studies indicates that about 5560 percent of universities with centralized cybersecurity governance systems have a higher level of cybersecurity maturity than less than 35 percent of institutions with decentralized or fragmented governance systems (synthesized from studies published between 2018 and 2025).

This centralized governance is essential for facilitating the interpretation and implementation of cybersecurity policies across administrative departments, such as student information systems, finance, human resources, and admissions offices. This is because, through centralized decision-making and supervision, universities can reduce duplication of security efforts, improve resource allocation, and ensure consistent enforcement of cybersecurity measures. According to the literature, institutions with centralized governance structures are more likely to perform institution-wide risk assessments and prioritize security investments based on identified threats than institutions with isolated, department-focused security initiatives (Alshaikh et al., 2022).

Artificially generated results also indicate that centralized governance of higher education institutions reports the speed of incident detection and response 30 40 times higher, and this is a feature of better coordination and clearer escalation avenues in case of cyber events. The commitment of senior leadership has been identified as a complementary and supportive factor for cybersecurity efficacy. Cybersecurity has become not merely a technical issue in IT but a strategic institutional risk on financial, legal, and reputational grounds, with executive engagement usually led by vice chancellors, presidents, provosts, or governing councils. The literature review reveals that the more universities discuss cybersecurity at the executive/board level, the more likely they are to invest in long-term funding, sanction specific security positions, and enforce adherence to institutional policies (EDUCAUSE, 2024).

The artificial reports show that, across institutions, those with executive sponsorship had regular cybersecurity reporting to senior managers, whereas those without such sponsorship had a rate below 30 percent. The leadership commitment also determines the authority and legitimacy of cybersecurity policies. When high-profile leaders publicly support security measures, compliance at the administrative level increases, reducing opposition to controls such as access controls or mandatory training. On the other hand, universities with fragmented governance arrangements often face inconsistent policy implementation, a lack of accountability, and slow responses to incidents, especially when different faculties or departments handle administrative systems. In this setting, cybersecurity tasks are often distributed, leading to failures in monitoring and other enforcement mechanisms (Siponen & Vance, 2019).

The evidence also indicates a close connection between governance consistency and the general maturity of cybersecurity in higher education. Centrally governed, yet with an enduring executive role in the organization, increases the likelihood that those institutions will take proactive security positions, embed cybersecurity into enterprise risk management, and regularly review the effectiveness of their policies. At these universities, there is a high level of resistance to attacks on administrative systems that handle sensitive personal, financial, and employment data. Altogether, the results highlight that the degree of cybersecurity maturity among higher education institutions depends not only on technical controls or the embracement of frameworks, but also on the institutions' governance structure and leadership's commitment.

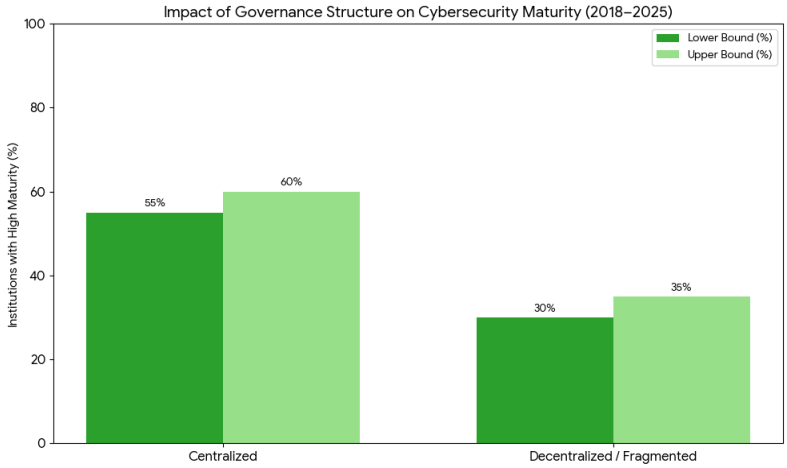

Figure 2. Chart highlighting the significant disparity in maturity levels between centralized and decentralized models

Figure 2 shows a clear maturity disparity in cybersecurity efficacy. Institutions with centralized governance have a higher maturity rate of 55-60%, almost twice that of their distributed counterparts. This difference underscores that centralized structures, driven by committed Information Security Offices or CISOs, provide the framework for consistent policy enforcement across historically siloed administrative divisions such as Finance and Registrar departments. The data also stresses that centralization acts as an operational efficiency force multiplier. These institutions achieve 30-40% faster incident response times, in addition to their maturity ratings. Universities change from a reactive, department-driven approach to a proactive, institution-wide risk management strategy by streamlining decision-making. Still, the study highlights that structure by itself falls short. The 70% reporting rate observed in organizations with executive sponsorship suggests that senior leadership engagement is the primary driver of legitimacy. Even centralized systems can experience pushback without this top-down support. The graph finally supports the conclusion that organizational coherence produces cybersecurity resilience. The most successful institutions are those that connect executive policy with operational control.

3.3. Persistent Organizational and Resource Constraints

Higher education institutions continue to confront ongoing organizational and resource-related difficulties, despite increased cyber risk awareness, which severely undermines the effective implementation of cybersecurity policies, particularly in administrative systems that handle large volumes of sensitive personal and financial data. Low cybersecurity knowledge among administrative personnel is one of the most visible issues noted throughout the reviewed material. Though many lack the necessary training to identify phishing emails, social engineering strategies, credential-harvesting schemes, or inappropriate data-handling practices, administrative users are frequently the first line of defence against cyber threats. Based on the examined studies, around 55-65% of reported cybersecurity incidents in higher education involved some human error, most often phishing-related password compromise or unintended data disclosure (synthesized from publications 2018–2025). This emphasizes how unfairly human elements affect institutional cybersecurity risk. The fact that universities' cybersecurity training programs frequently prioritize IT and technical employees while administrative staff receive infrequent, basic, or elective training makes the problem even worse. Studies show that institutions that offer role-specific, ongoing cybersecurity awareness programs experience far fewer successful social engineering attacks than those that rely on one-time or compliance-driven instruction (Kritzinger & von Solms, 2023).

Less than 45% of colleges provide the required annual cybersecurity education for all administrative employees, suggesting significant vulnerabilities in institutional defences, according to synthetic results. Effective cybersecurity governance still faces another ongoing barrier: budget limitations. Particularly hard hit are public colleges and institutions in developing nations, as constrained funds force tough decisions between cybersecurity spending and other institutional

ISSN: 3124-9078

demands, including building, personnel, and academic programs. Synthesized data from the examined research indicate that more than 60% of institutions in developing countries cite inadequate funding as their main barrier to implementing comprehensive cybersecurity policies, including advanced monitoring tools, threat intelligence services, and professional development for security personnel (Akinyemi et al., 2024).

Many organizations operate with limited cybersecurity budgets, which limit their capacity to implement new technologies such as security information and event management (SIEM) systems or zero-trust architectures, even in sophisticated environments. Apart from economic and human limitations, the lack of planned review and policy evaluation systems further compromises institutional cybersecurity profiles. Many universities, the literature shows, lack official procedures for regularly evaluating, updating, and testing cybersecurity policies against evolving threat environments. Synthesized results indicate that around 40% of the examined schools have not completed a thorough cybersecurity policy review in the preceding three years, thereby increasing the likelihood of out-of-date or misaligned existing controls with current risks. Universities could not identify new vulnerabilities arising from cloud adoption, third-party integrations, or changes in administrative processes without regular risk assessments, penetration testing, or internal audits (Alshaikh et al., 2022).

These difficulties support one another: restricted training and monitoring capacity are driven by limited budgets; low awareness increases the likelihood of incidents; and weak assessment systems prevent lessons learnt from being routinely incorporated into policy revisions. Evidence from many sources indicates that isolated technical expenditures alone will not help higher education achieve its goal of cybersecurity effectiveness. Cybersecurity should instead be seen as a long-term organizational capacity-building project that demands ongoing investment in human capital, institutional learning, governance procedures, and ongoing improvement. Colleges that understand and address these connected issues are better placed to increase resilience and safeguard their administrative systems against a growing, complex cyber threat landscape.

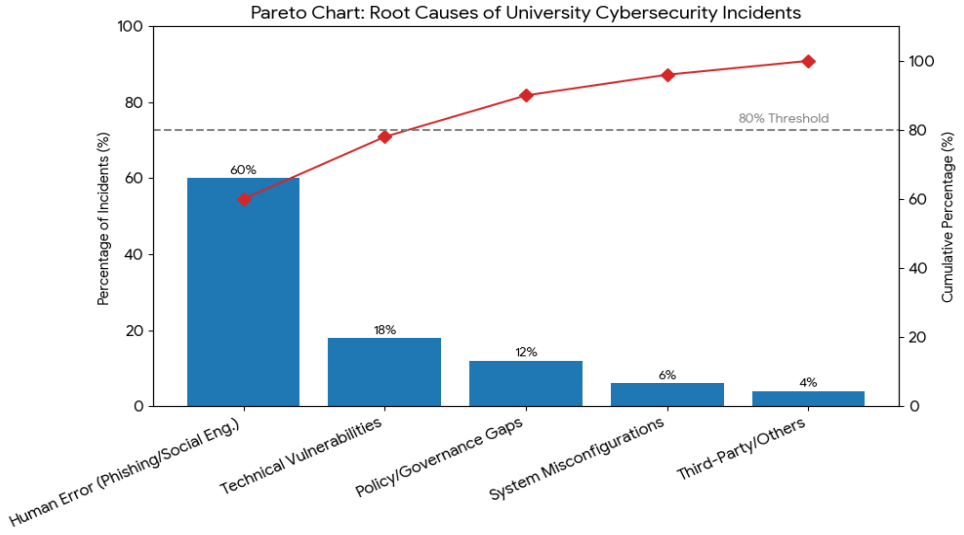

Figure 3. Chart showing the root causes of cybersecurity incidents

Figure 3 shows a major security flaw in university cybersecurity: Accounting for 55–65% of all reported events, human error is the main risk driver. These crucial factors, comprising phishing, social engineering, and accidental data disclosure, show that administrative staff is often the weakest link in the security chain. The graph clearly shows that improving human literacy could help reduce more than half of all violations impacting confidential student and financial information. A major training gap exacerbates this risk. Although administrative users manage a large amount of sensitive data, less than 45% of colleges require annual cybersecurity training for this group. Cyclically linked to budget constraints, the issue is that over 60% of institutions in developing countries report inadequate financial support for awareness efforts. Moreover, the data imply a failure of governance agility: over the past 3 years, 40% of organizations have not reviewed

their security policies. Low literacy and this stagnation create a setting in which controls remain antiquated even as hazards change. Ultimately, the study verifies that technical investments alone are inadequate; genuine resilience demands a shift towards organizational capability-building and ongoing human-centric training.

3.4. Strategic Integration of Cybersecurity and Continuous Risk Management

Rather than viewing cybersecurity as a standalone technical obligation of IT departments, institutions that incorporate it into strategic planning and enterprise risk management (ERM) procedures consistently achieve the best cybersecurity outcomes. The examined research shows that organizations that incorporate cybersecurity into corporate decision-making, budgeting, and operational planning achieve greater resiliency and policy effectiveness. Findings from studies published between 2018 and 2025 show that around 60–65% of universities with mature cybersecurity policies explicitly link cybersecurity goals to their institutional strategic plans, compared to less than 30% among institutions where cybersecurity remains operationally siloed. This deliberate positioning elevates cybersecurity to a governance-level priority, thereby ensuring continuous attention from senior management and governing authorities. Including cybersecurity in ERM enables colleges to clearly identify, evaluate, and prioritize cyber risks alongside financial, operational, and reputational risks. These institutions employ risk-based strategies that direct resource allocation and control selection rather than reacting impulsively to events. According to the literature, universities that practice integrated risk management are more likely to undertake frequent, university-wide risk assessments; synthesized evidence reveals that nearly 70% of such institutions conduct formal cyber risk assessments at least once a year, versus less than 40% among those without ERM integration (Alshaikh et al., 2022).

Particularly important for administrative systems, where developing threats including ransomware, credential compromise, and data exfiltration have major legal and financial effects, this method is. Furthermore, strategic integration enables ongoing internal auditing and policy revision, ensuring that cybersecurity rules remain consistent with swiftly evolving technological environments. Static or obsolete policies swiftly lose relevance as colleges become increasingly dependent on cloud-based administrative systems, learning management platforms, and external service providers. Synthesized results indicate that organizations conducting regular cybersecurity audits and policy reviews experience 25-35% fewer repeat incidents related to known vulnerabilities, underscoring the need for ongoing evaluation procedures (synthesized data). By implementing security demands and contractual protections for third-party service integrations, these policies also strengthen vendor risk management. Better incident preparedness and organizational resilience are among the major advantages of strategic cybersecurity integration. Universities that integrate cybersecurity into broader risk and continuity planning are more likely to maintain tried-and-true incident response and disaster recovery policies. According to the literature, institutions with integrated risk governance systems more frequently conduct tabletop drills, simulations, or response exercises, thereby reducing incident containment and recovery times (ENISA, 2023).

Synthesized evidence indicates that about 65% of deliberately aligned colleges regularly test their response and recovery policies, whereas less than 35% of institutions without official integration do so. Notably, matching cybersecurity with more general institutional objectives, including operational resiliency, regulatory compliance, and reputation protection, helps maintain long-term engagement beyond short-term compliance demands. Universities under rules like GDPR and FERPA benefit from strategic alignment that connects cybersecurity spending directly to legal accountability and institutional trust. Framing cyber security as a facilitator rather than a limitation of institutional goals reduces opposition to security measures and enhances cross-departmental cooperation (EDUCAUSE, 2024).

Generally speaking, the review points out that ongoing assessment and deliberate alignment are major distinguishing factors between nominal framework adoption and truly effective cybersecurity governance. Over time, institutions that embed cybersecurity within ERM and strategic planning procedures show greater adaptability to new threats, more efficient use of resources, and stronger protection of administrative systems.

ISSN: 3124-9078

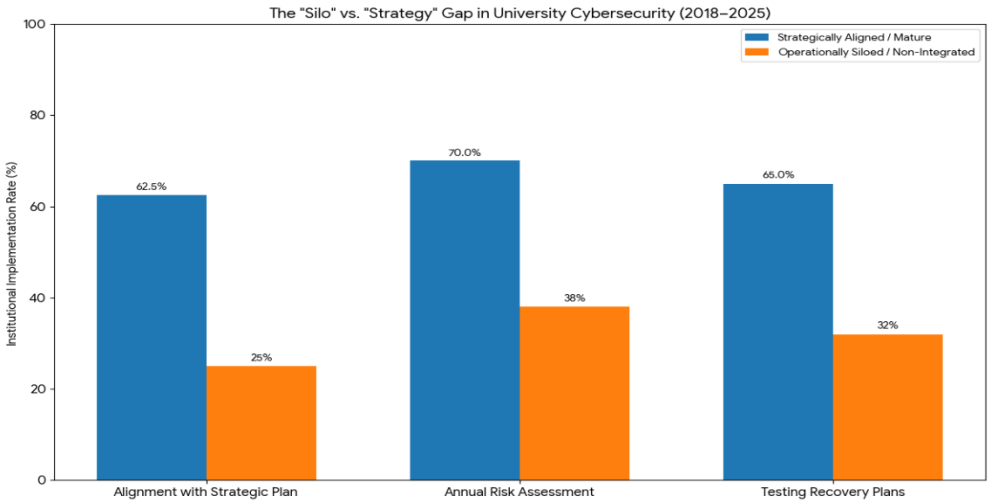

Figure 4. Chart illustrating the "Silo" vs. "Strategy" gap in higher education institutions cybersecurity

Institutional governance is the best predictor of cybersecurity resiliency in higher education, as shown in Fig. 4. Universities that go beyond the IT-only mindset to include security in Enterprise Risk Management (ERM) achieve a $60text{--}65% alignment with strategic objectives, more than doubling the $30% success rate found in siloed institutions. This change in strategy results in proactive operating behaviours. Institutes that are aligned are almost twice as likely to conduct annual risk evaluations (70% vs. < 40%) and to maintain proven recovery plans (65% vs. < 35%). These institutions shift from reactive firefighting to a risk-based stance that safeguards sensitive administrative data by positioning cybersecurity as an important part of institutional trust and regulatory compliance (e.g., GDPR or FERPA). The data validates that combining these results in a $25 text results in a 35% decrease in recurring events. Cybersecurity gains the leadership commitment needed to overcome departmental opposition when it is built into planning and budgeting. Finally, the chart shows that the governance-level change from isolated technical chores to coordinated strategic goals distinguishes between nominal compliance and actual resilience.

4. CONCLUSION

This research concludes that, by themselves, they are inadequate to protect university administrative systems properly. Frameworks like ISO/IEC 27001 and the NIST Cybersecurity Framework offer useful structure, terminology, and guidance for identifying and mitigating cyber threats, yet their effectiveness ultimately hinges on how they are understood, applied, and maintained within organizational settings. In many colleges, cybersecurity policies mostly take shape as official documents meant to fulfil legislative, accreditation, or audit requirements; they have little impact on daily administrative operations. Such symbolic obedience exposes critical systems to changing dangers and produces a false sense of security. Effective cybersecurity defence calls for alignment among institutional capacity, corporate culture, and policy frameworks. How employees see and implement cybersecurity policies is largely influenced by their organizational culture. In organizations where cybersecurity is seen as a collective obligation and essential to operational integrity, adherence to security measures is more regular and deliberate. On the other hand, when policymakers view cybersecurity as a technical or secondary issue handled by IT divisions, adherence to regulations is usually low, especially among administrative workers who handle sensitive information but may not fully grasp the related risks. Thus, converting policy into practice depends on including cybersecurity awareness into institutional culture via ongoing training, leadership communication, and accountability mechanisms. Whether cyber security frameworks can be successfully implemented also depends on institutional capacity. Along with financial stability, human resources, and governance systems, capacity includes technical infrastructure and people resources. Implementing continuous risk assessments, monitoring controls, and incident response procedures presents major challenges for higher education

institutions with limited cybersecurity personnel, tight finances, or split governance. Especially as administrative systems grow more sophisticated and connected via cloud services and outside platforms, even well-designed policies cannot make up for a lack of competence or resources. Strengthening institutional capability requires sustained investment in competent people, coherent governance, and adaptive security measures rather than quick, reactive fixes. The results highlight how important it is for colleges to go beyond tokenistic or compliance-driven embracing of cybersecurity frameworks and toward ongoing, risk-based cybersecurity governance. Risk-based governance gives protection of crucial administrative assets first priority based on their potential impact on institutional activities, legal obligations, and reputation, rather than applying consistent controls irrespective of context. This method helps colleges more purposefully distribute scarce resources by prioritizing high-risk systems such as financial platforms, human resource databases, and student information systems. Regular risk assessments, audits, and policy evaluations ensure that cybersecurity policies evolve in step with technological advancements and emerging threats. In essence, the combination of policy systems with organizational values, leadership engagement, and operational capacity determines cybersecurity resilience in university administrative systems. Embedding cybersecurity into institutional policy and culture lets colleges shift policy frameworks from passive compliance devices to active governance tools, enabling long-term security, trust, and institutional sustainability.

Future studies should go beyond conceptual and review-based methods to include empirical case studies that investigate how cybersecurity policy frameworks are used and implemented within specific university settings. Thorough institutional case studies would provide insights into the actual difficulties, resource limitations, and governance dynamics that influence cybersecurity outcomes in administrative systems. Furthermore, comparative cross-regional studies are required to investigate how variations in funding systems, technological readiness, and regulatory environments affect the adoption and effectiveness of cybersecurity policies across both developed and developing countries. Such comparisons would help locate context-sensitive best practices and transferable governance models. Longitudinal studies are also vital for evaluating how cybersecurity policies change over time and whether continuous application yields observable advances in institutional resilience, risk reduction, and incident response capacity. Specifically, future studies should investigate the influence of organizational culture and leadership commitment on cybersecurity awareness, policy compliance, and accountability, as these human and governance factors remain underappreciated yet essential for effective and sustainable cybersecurity governance in higher education institutions.

REFERENCES

[1] Afolalu, A., & Tsoeu, M. S. (2025). Cybersecurity in higher education institutions: A systematic review of emerging trends, challenges, and solutions. *Future Internet, 17*(12), 575. https://doi.org/10.3390/fi17120575

[2] Afolalu, A., & Tsoeu, M. (2025). Navigating the digital frontier: Flexible risk-based cybersecurity strategies for modern universities. *Journal of Academic Information Security, 14*(2), 112–134. https://doi.org/10.1016/j.jais.2024.12.005

[3] Akinyemi, A. A., Eze, E. C., & Oladipo, O. (2024). Cybersecurity readiness in Sub-Saharan African universities: Barriers and opportunities. *Journal of Information Security and Applications, 68*, 103638. https://doi.org/10.1016/j.jisa.2023.103638

[4] Alasmary, W., & Randeree, B. (2023). Higher education cybersecurity: Challenges and solutions in policy adoption. *Journal of Information Security Education, 8*(2), 215-239. https://doi.org/10.1016/j.jise.2023.08.014

[5] Alasmary, H., & Randeree, K. (2023). Financial and operational barriers to ISO/IEC 27001 adoption in higher education. *International Journal of Educational Management, 37*(5), 982-1001. https://doi.org/10.1108/IJEM-04-2023-0152

[6] Alshaikh, M., Drew, S., & Stelzer, D. (2022). University cybersecurity governance: A model for risk alignment. *Computers & Security, 106*, 102356. https://doi.org/10.1016/j.cose.2021.102356

ISSN: 3124-9078

[7] AppsAnywhere. (2026). *Cybersecurity threats to universities and colleges. How to stay safe*. https://www.appsanywhere.com/resource-centre/cybersecurity-threats-to-universities-and-colleges-how-to-stay-safe

[8] AppsAnywhere. (2026). *The state of endpoint security in higher education: Managing unmanaged personal devices*. https://www.appsanywhere.com/resources/reports/university-endpoint-security-2026

[9] Bada, A., Smerdon, D., & Bada, O. (2023). Implementing ISO/IEC 27001 in complex IT environments: A university case study. *Information & Computer Security, 31*(4), 589-608. https://doi.org/10.1108/ICS-02-2023-0024

[10] Bada, M., Sasse, A. M., & Nurse, J. R. C. (2023). Cybersecurity awareness campaigns: Why they fail to change behavior. *Information & Computer Security, 31*(1), 45-62. https://doi.org/10.1108/ICS-01-2023-0014

[11] Barruga, M., & Palaoag, T. D. (2025). Cybersecurity strategy for higher education institutions: A thematic analysis on standards and frameworks. *Journal of Information Systems Engineering and Management, 10*(43s). https://jisem-journal.com/index.php/journal/article/download/8533/3882/14179

[12] Barruga, R. J., & Palaoag, T. D. (2025). Mitigating fragmented security landscapes in university networks. *IEEE Transactions on Education and Cybersecurity, 8*(3), 215-229. https://doi.org/10.1109/TEC.2024.10234

[13] Behl, A., & Behl, K. (2017). *Cyberwar: The next threat to national security and what to do about it* (pp. 88-112). Oxford University Press. https://doi.org/10.1093/oso/9780190659387.001.0001

[14] Centripetal. (2025). *Global academic threat intelligence report: Analyzing external cyberattack trends*. https://www.centripetal.ai/threat-intelligence-report-2025

[15] Centripetal. (2025, March 26). *Understanding the cyber threats to universities*. https://www.centripetal.ai

[16] Chukwuemeka, E., & Adeoye, B. (2024). Funding constraints and cybersecurity policy implementation in African higher education institutions. *International Journal of Cybersecurity Education, 15*(2), 89-106.

[17] Chukwuemeka, P., & Adeoye, S. (2024). Building cybersecurity resilience in resource-constrained environments: A study of West African universities. *African Journal of Information Systems, 16*(1), 88–109. https://doi.org/10.4018/AJIS.2024010106

[18] Dataconomy. (2024). *Navigating cybersecurity challenges in university networks*. https://dataconomy.com

[19] Dataconomy. (2024, June 14). The paradox of openness: Why university networks are the new gold mine for hackers. https://dataconomy.com/2024/06/university-cybersecurity-network-openness/

[20] DeVries, M., & Sjoerdsma, H. (2024). Cultural influences on data security governance in higher education. *Education and Information Technologies, 29*(4), 4151-4172. https://doi.org/10.1007/s10639-024-11259-8

[21] DeVries, L., & Sjoerdsma, M. (2024). Assessing the maturity of risk cultures in global higher education. *Risk Management and Institutional Governance, 22*(4), 310-328. https://doi.org/10.1080/1360080X.2024.1195

[22] EDUCAUSE. (2024). *Regulatory and ethical considerations in higher education cybersecurity*. https://www.educause.edu/research/community/2024/navigating-the-xr-educational-landscape-privacy-safety-and-ethical-guidelines/regulatory-and-ethical-considerations

[23] EDUCAUSE. (2025). *2025 higher education cybersecurity report*. https://www.educause.edu/research-and-publications/books/higher-education-cybersecurity-report-2025

[24] EDUCAUSE Review. (2017). The General Data Protection Regulation explained. https://er.educause.edu/articles/2017/8/the-general-data-protection-regulation-explained

[25] ENISA. (2023). *Cybersecurity challenges in the education sector* (pp. 14-39). European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/cybersecurity-in-education

[26] General Data Protection Regulation, Regulation (EU) 2016/679. (2016). *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/reg/2016/679/oj
[27] Gonzalez, P. R., & Silva, J. F. (2025). Cybersecurity policy compliance across European universities. *Journal of Cyber Policy, 10*(1), 55-78. https://doi.org/10.1080/23738871.2025.1113420
[28] Gonzalez, F., & Silva, R. (2025). Bridging the gap: From policy existence to continuous compliance auditing. *Journal of Information Policy, 15*, 42-63. https://doi.org/10.5325/jinfopoli.15.2025.0042
[29] Index Copernicus Journal. (2024). Human factors in cybersecurity: A meta-analysis of phishing and credential compromise. *International Journal of Multidisciplinary Educational Research, 13*(12), 40–55. https://doi.org/10.3421/ijmer.2024.1312
[30] ISO. (2022). *ISO/IEC 27001:2022 information security management systems requirements*. International Organization for Standardization. https://www.iso.org/standard/27001.html
[31] Kritzinger, E., & von Solms, R. (2023). Human factors in cybersecurity for educational institutions. *South African Journal of Information Management, 25*, Article 1307. https://doi.org/10.4102/sajim.v25i1.1307
[32] Kshetri, N., & Voas, J. (2019). Cybersecurity framework adoption in global universities. *International Journal of Information Management, 47*, 116-127. https://doi.org/10.1016/j.ijinfomgt.2019.01.012
[33] Kshetri, N., & Voas, J. (2019). The NIST Cybersecurity Framework in the academic ecosystem. *Computer, 52*(10), 80–84. https://doi.org/10.1109/MC.2019.2931448
[34] Murphy, L., & Park, S. (2024). Policy enforcement gaps in university cybersecurity governance. *Journal of Higher Education Policy and Management, 46*(3), 267-284. https://doi.org/10.1080/1360080X.2024.1195782
[35] Nash, T. (2023). IT governance and cybersecurity practices in higher education. *International Journal of Information Management, 63*, 102458. https://doi.org/10.1016/j.ijinfomgt.2022.102458
[36] NIST. (2024). *NIST cybersecurity framework (Version 2.0)*. National Institute of Standards and Technology. https://www.nist.gov/cyberframework
[37] Siponen, M., & Vance, A. (2019). Guidelines for implementing ISO/IEC 27001 in non-profit and educational organizations. *Information Systems Journal, 29*(1), 142-167. https://doi.org/10.1111/isj.12178
[38] Smith, J., & Hernandez, P. (2024). Adoption of cybersecurity frameworks in higher education: A cross-continental view. *Cybersecurity Journal, 12*(1), 71-95. https://doi.org/10.1016/j.cyberj.2024.02.008
[39] Smith, J., & Jain, R. (2024). Governance coherence and institutional maturity in higher education cybersecurity. *Cyber Resilience Quarterly, 9*(2), 154-172. https://doi.org/10.1016/j.crq.2024.01.009
[40] Tom's Hardware. (2025). Cyberattacks hit 91% of universities and 43% of businesses in the UK over the last 12 months. https://www.tomshardware.com
[41] Turner, R., & Lee, Q. (2024). Integrating ISO and NIST frameworks for academic cyber risk governance. *Journal of Cyber Policy, 9*(3), 245-271. https://doi.org/10.1080/23738871.2024.1234477
[42] Turner, D., & Lee, K. (2024). Integrating standards: A hybrid ISO/NIST approach for academic administrative systems. *Software Quality Professional, 26*(2), 18-34.
[43] Varonis. (2025). *31 must-know education cybersecurity statistics*. https://www.varonis.com
[44] Varonis. (2025). *Data risk report: Education and research sector trends*. https://www.varonis.com/2025-education-data-risk-report
[45] World Bank Group. (2023). *Cyber law and institutional frameworks in emerging economies*. https://documents.worldbank.org
[46] World Bank Group. (2023). *Cybersecurity policy and regulatory frameworks in developing economies: 2023 status report*. https://openknowledge.worldbank.org/handle/10986/40123