Cybersecurity and Governance in Online Education: Addressing Policy Gaps in Protecting Students' Digital Identities

Chukwudum Collins Umoke
Department of Science Education,
Alex Ekwueme Federal University Ndufu-Alike, Ebonyi State.
umoke.chukwudum@funai.edu.ng

Sunday Odo Nwangbo
Department of Political Science,
Alex Ekwueme Federal University Ndufu-Alike, Ebonyi State.
snwangbo@gmail.com

Oroke Abel Onwe
Department of Computer Science Education,
Ebonyi State College of Education, Ikwo orokeabel@gmail.com

Kennedy Ololo
Department of Sociology
Alex Ekwueme Federal University Ndufu Alike, Ebonyi State, Nigeria
kenololo@yahoo.com
DOI: 10.56201/ijssmr.vol.11no4.2025.pg499.515

Abstract
The expansion of online education has introduced new forms of digital vulnerability, particularly in relation to student data privacy and cybersecurity. While educational technologies offer greater access and personalization, they also expose learners—especially minors and marginalized students—to data breaches, surveillance, and algorithmic exploitation. Existing policy frameworks such as FERPA, COPPA, and GDPR offer limited protection, failing to address cloud-based architectures, third-party vendors, and behavioral analytics embedded in digital learning environments. This study develops the Student-Centric Cybersecurity Governance Model (SCCGM)—a conceptual framework designed to prioritize student digital identity protection through integrated cybersecurity strategy and ethical governance. Using a qualitative documentary methodology, the study synthesizes literature and policy insights across four domains: systemic threat vectors, privacy and data governance ethics, national and institutional policy gaps, and cybersecurity best practices. Findings reveal a fragmented governance landscape in which regulatory inaction and underutilization of global frameworks leave students vulnerable to preventable cyber threats. The SCCGM offers a structured model to guide institutions, policymakers, and educators in developing transparent, rights-based, and future-ready cybersecurity protocols. As online learning becomes a core component of global education, this model serves as a roadmap for aligning digital transformation with student protection and educational equity.

Keywords: *Digital Identity, Cybersecurity governance, Data Privacy, Online learning, Policy Gaps, Student-Centric Cybersecurity, Governance Model*

Introduction

The global shift to online education has revolutionized pedagogical delivery, enabling flexible, scalable, and technologically mediated learning environments. This transition, while transformative, has surfaced a parallel crisis in digital security, with educational institutions increasingly becoming prime targets for cyberattacks (Sophos, 2024; MySanAntonio, 2025). As digital platforms become the central medium for student engagement, the integrity of student digital identities—comprising personal data, behavioral traces, and biometric records—faces unprecedented threats (Kelso et al., 2024; Chantal et al., 2023). These risks are amplified by the expansion of EdTech ecosystems where data collection, algorithmic profiling, and opaque third-party integrations often operate without robust regulatory or ethical oversight (ASCD, n.d.; New America, 2024). Cybersecurity in education remains severely under-prioritized, despite the sector's vulnerability to ransomware, phishing, and insider threats (Virtru, 2021; LevelBlue, 2024). Unlike corporate enterprises, most educational institutions lack centralized security governance, comprehensive response frameworks, or the financial bandwidth to adopt and operationalize internationally recognized cybersecurity protocols such as the NIST Cybersecurity Framework or ISO/IEC 27001 (Bondoc & Malawit, 2020; Kumar et al., 2024). The decentralized nature of K–12 and higher education governance exacerbates these gaps, as institutions often operate in silos without coordinated standards or inter-agency support systems (Fouad, 2021; Lewis & Crumpler, 2019).

Compounding these vulnerabilities is the limited reach of existing data privacy laws. The Family Educational Rights and Privacy Act (FERPA) and the Children's Online Privacy Protection Act (COPPA) offer only fragmented protections, and their provisions fail to adequately govern data collected through biometric surveillance, learning analytics, or behavioral tracking in cloud-based systems (Sun, 2023; AP News, 2023; ASCD, n.d.). While the European Union's General Data Protection Regulation (GDPR) has advanced more robust protections, its implementation within education remains inconsistent and lacks specificity for EdTech contexts (Salminen et al., 2023).

Equally pressing are the ethical implications surrounding consent, autonomy, and agency. Students, particularly minors and marginalized populations, often have little to no understanding of how their data is collected, used, or stored—let alone the capacity to challenge unethical or exploitative practices (Mutimukwe et al., 2021; Kelso et al., 2024). As monitoring software becomes embedded in online proctoring and attendance systems, student surveillance is being normalized under the guise of security or academic integrity, raising serious concerns about equity, psychological safety, and digital rights (Chantal et al., 2023). At the institutional level, these challenges are met with uneven preparedness. While some universities have adopted multi-stakeholder governance models or partnered with national cybersecurity response teams (e.g., EduCERT), many still lack basic incident response protocols or security awareness training for staff and students (Otoom et al., 2024; Petersen et al., 2020). Furthermore, despite the availability of comprehensive frameworks such as NICE, CyBOK, and CSEC2017, curricular integration of cybersecurity and digital ethics remains limited across most educational systems (Hajny et al., 2021; Langner et al., 2023). This curricular void contributes to a generational skills gap, weakening institutional resilience and national cybersecurity capacity alike (Limnell et al., 2023; Crabb et al., 2024).

These conditions underscore a fundamental misalignment between technological advancement and regulatory adaptation. While digital learning infrastructures are scaling rapidly, governance structures remain reactive, fragmented, and frequently outpaced by innovation (Fouad, 2021; Kumar et al., 2023). Without a conceptual framework that synthesizes threat vectors, regulatory blind spots, institutional best practices, and student-centric ethics, the digital future of education risks becoming an extractive, exclusionary, and insecure domain. This article responds to that gap by developing the **Student-Centric Cybersecurity**

Governance Model (SCCGM)—a conceptual framework grounded in documentary analysis of scholarly, regulatory, and technical sources. The SCCGM centers on student digital identity protection and is organized around four interrelated domains: (1) threat vectors and systemic vulnerabilities, (2) privacy and data governance ethics, (3) policy and regulatory gaps, and (4) cybersecurity governance and best practices. The model positions these domains as mutually reinforcing levers for building resilient, inclusive, and ethically grounded digital education systems.

The purpose of this paper is to critically examine how cybersecurity and data governance structures in education can be reoriented to prioritize student rights, agency, and protection. It contributes to existing scholarship by offering a holistic, scalable framework that addresses not only technical implementation but also ethical responsibility and regulatory reform. As online learning becomes an enduring pillar of global education, this framework aims to inform policy development, institutional strategy, and curriculum design with a strong emphasis on accountability and equity.

The remainder of the paper is structured as follows. The **literature review** synthesizes insights across four thematic domains related to cybersecurity threats, privacy ethics, governance gaps, and institutional frameworks. The **conceptual framework** section introduces and describes the SCCGM, detailing the relationships between its core components. The **methodology** explains the qualitative, documentary approach used to identify and analyze the literature. The **findings and discussion** articulate how insights from each theme converge to support the model's relevance, while also exploring the broader implications for educational institutions and policymakers. Finally, the **conclusion and future studies** section summarizes key arguments and offers pathways for advancing research, practice, and policy in student-centered cybersecurity governance.

Literature Review

Threat Landscape and Vulnerabilities in Online Education

The digital transformation of education has introduced not only pedagogical innovation but also an expanded threat surface vulnerable to cyber exploitation. As online learning becomes embedded in educational delivery, schools and universities have emerged as soft targets for increasingly sophisticated cyberattacks. These threats compromise both institutional operations and, more critically, the integrity of students' digital identities. Ransomware attacks on educational institutions have escalated dramatically. According to recent findings, 63% of lower education and 66% of higher education institutions were impacted by ransomware in the past year alone, leading to widespread data encryption, operational downtime, and extortion demands (Sophos, 2024). These incidents are not only disruptive but often result in unauthorized access to student data, exposing sensitive personal information to cybercriminal networks.

Phishing attacks represent another significant threat vector. Spoofed emails mimicking legitimate platforms such as Google Classroom or Microsoft Teams have deceived students and staff into disclosing login credentials and other personal details (Prey Project, 2024). This form of social engineering capitalizes on user trust and low cybersecurity awareness, especially among younger learners who are more susceptible to deception. Data breaches further illustrate the fragility of current online education infrastructures. In one high-profile case, a breach affected nearly 800,000 students in Texas, revealing names, addresses, and social security numbers (MySanAntonio, 2025). Such breaches often stem from lax security configurations and insufficient encryption protocols in student information systems. The rapid adoption of remote learning technologies has compounded these challenges. Educational institutions frequently deploy virtual desktops and online classrooms without adequate vetting or security auditing, creating vulnerabilities that adversaries can exploit (EdTech Magazine, 2024). These

oversights expose schools to credential harvesting, session hijacking, and unauthorized surveillance.

Compounding these technical vulnerabilities is a widespread lack of cybersecurity literacy among students. Many learners are unaware of basic threat indicators such as suspicious links or insecure network connections. According to Western Governors University (2024), this knowledge gap makes students prime targets for malware, phishing, and identity theft, especially when using personal devices that lack enterprise-grade protection. The use of personal devices—often unregulated—amplifies institutional risk. Bring Your Own Device (BYOD) policies, while cost-effective, introduce endpoint security issues, as personal hardware may lack updated antivirus software or firewall protection (Virtru, 2021). These devices become potential vectors for malware propagation and unauthorized network access. Insider threats also merit attention. Unauthorized access by former students, disgruntled staff, or even current users can compromise system integrity, especially in the absence of role-based access controls and session monitoring tools (LevelBlue, 2024). Institutions frequently lack the internal auditing capacity to detect these breaches in real time.

Beyond technical gaps, many educational institutions operate without comprehensive data protection policies. This regulatory vacuum results in inconsistent security practices, delayed incident responses, and prolonged exposure periods for affected students (Student Privacy Compass, n.d.). When cybersecurity events do occur, disclosure is often delayed or incomplete, obstructing mitigation efforts and eroding stakeholder trust (The 74, 2025). The integration of third-party applications adds another layer of risk. These tools, often used to enhance learning experience, are rarely subjected to the same security scrutiny as institutional platforms. When third-party apps have weak authentication protocols or inadequate data handling policies, they create backdoors for cyber intrusions (Johns Hopkins University, 2024). The literature paints a picture of a fragmented and reactive cybersecurity ecosystem in online education. While threats such as ransomware, phishing, and data breaches are well-documented, institutional preparedness remains uneven. Without robust policies, cybersecurity training, and architectural safeguards, student digital identities will continue to be exposed to preventable risks. The absence of coherent threat mitigation strategies not only jeopardizes educational continuity but undermines student trust in digital learning environments.

Privacy, Consent, and Data Governance for Students

As educational institutions increasingly depend on digital platforms to facilitate learning, concerns surrounding student privacy, consent, and data governance have become central to debates on digital rights and educational ethics. The collection, storage, analysis, and sharing of student data—often without meaningful oversight—have introduced profound legal, ethical, and operational risks. These risks are amplified in an environment where students are frequently unaware of how their data is used and where regulatory frameworks remain misaligned with emerging technological realities. The limitations of the Family Educational Rights and Privacy Act (FERPA) exemplify the inadequacy of legacy legislation in the digital age. Originally enacted in 1974 to protect student academic records, FERPA has become increasingly porous, allowing educational institutions to share student data with third-party vendors without explicit consent (ASCD, n.d.). This legal loophole has eroded parental and student control over data and has failed to address modern surveillance-based educational technologies. In K–12 settings, the absence of comprehensive data governance policies has led to inconsistent practices in data handling. EdTech Magazine (2024) notes that many school districts operate with little or no centralized oversight regarding data collection, storage, and third-party access, increasing the risk of privacy breaches. This institutional inconsistency undermines accountability and leaves data security decisions to individual administrators or IT staff.

The challenges extend to higher education, where contractual power imbalances make it difficult for universities to hold educational technology (EdTech) vendors accountable for privacy violations. Kelso et al. (2024) point out that universities often lack visibility into the internal data processing operations of EdTech companies, resulting in diminished leverage to enforce ethical data usage. This asymmetry places students at heightened risk of surveillance, profiling, and unauthorized data exploitation. Learning analytics—while valuable for personalizing education—raise complex privacy concerns. These systems track student behaviors, responses, and performance metrics, aggregating data into predictive models that are often opaque and prone to misinterpretation. Mutimukwe et al. (2021) argue that such practices risk undermining student autonomy and can deter open engagement when students are aware of being constantly monitored.

Efforts to strengthen regulatory protections are underway. For instance, the Federal Trade Commission has proposed updates to the Children's Online Privacy Protection Act (COPPA) to limit data retention and restrict behavioral advertising in digital learning environments (AP News, 2023). These proposed changes reflect growing awareness that children require heightened protections in AI-driven, data-intensive platforms. However, privacy concerns are not limited to minors. Surveillance technologies such as student monitoring software have become normalized in educational environments. Though often framed as safety measures, these tools have disproportionately targeted marginalized students and raised red flags regarding informed consent and psychological well-being. The lack of opt-out options and transparency in these systems exacerbates ethical concerns.

Transparency, or the lack thereof, remains a recurring theme. Many online educational services fail to clearly communicate data collection practices or obtain meaningful consent from students and guardians. As noted by the U.S. Department of Education (2014), ambiguity in privacy statements and Terms of Service agreements prevents users from making informed decisions about their digital footprint in education. Cross-agency data governance has been recommended as a solution to fragmentation. NASBE (n.d.) emphasizes the need for shared protocols among education, health, and social service agencies to ensure responsible data sharing while safeguarding student privacy. This approach supports a holistic understanding of the student while reinforcing ethical boundaries on data use. Student agency remains at the heart of data governance reform. New America (2024) contends that privacy frameworks must empower students by granting them greater control over what data is collected, how it is used, and with whom it is shared. Without such provisions, educational data governance continues to function as a top-down surveillance model rather than a participatory rights-based system.

Finally, the collection of biometric data, such as facial recognition and keystroke dynamics used in online proctoring, introduces profound ethical dilemmas. Chantal et al. (2023) argue that students are frequently unaware of the extent to which biometric data is captured, stored, or shared, raising urgent questions about bodily autonomy and data permanence in digital learning contexts. Collectively, the literature reveals a data governance ecosystem in education that is reactive, fragmented, and ethically underdeveloped. While efforts to strengthen legal protections and introduce accountability mechanisms are gaining traction, much remains to be done to align educational technologies with the principles of consent, transparency, and student autonomy.

National and Institutional Policy Gaps

The proliferation of digital technologies in education has exposed significant regulatory shortfalls at both national and institutional levels. While online learning environments now form an integral part of global education systems, existing policies are often misaligned with the cybersecurity and privacy risks that students face. This disjunction results in an underregulated ecosystem where digital identities are inadequately protected, institutional

accountability is inconsistent, and student rights are poorly defined. One of the most pressing issues lies in the fragmentation of existing data protection laws. While the Family Educational Rights and Privacy Act (FERPA) in the U.S. and the General Data Protection Regulation (GDPR) in the EU offer foundational protections, both frameworks exhibit structural limitations when applied to modern, cloud-based educational ecosystems. As Sun (2023) notes, FERPA lacks robust consent mechanisms for third-party data sharing, while GDPR's implementation varies significantly across jurisdictions, leading to inconsistent levels of student protection. Despite the designation of cybersecurity academic centers by the U.S. National Security Agency, education policies related to cybersecurity remain largely uncoordinated. Crabb et al. (2024) highlight that many institutions lack alignment with national cybersecurity standards, resulting in a workforce that is inconsistently trained and underprepared for contemporary threats. This disconnect between policy intent and institutional capacity undermines both defensive readiness and curricular coherence.

The impact of **underfunding** is particularly acute. Financial constraints prevent many institutions—especially public K–12 systems and community colleges—from implementing basic cybersecurity protocols such as endpoint encryption, multi-factor authentication, and intrusion detection systems. As Watini et al. (2024) observe, these budgetary deficiencies expose student records to avoidable breaches and reduce the ability of institutions to respond to incidents effectively. Moreover, cybersecurity governance in higher education is frequently marginalized. Institutions often treat cybersecurity as a technical problem relegated to IT departments, rather than as an enterprise-wide strategic priority. Fouad (2021) argues that this narrow framing ignores the sector's broader responsibilities within national cybersecurity strategies and results in a failure to anticipate or respond to system-wide vulnerabilities.

Internationally, there is no universally accepted framework for cybersecurity education or protection within the K–12 environment. Malecki (2018) points out that while many national strategies emphasize digital innovation, they often neglect foundational aspects such as digital ethics, privacy literacy, and safe digital citizenship. The absence of national curricular mandates perpetuates a generation of students who are digitally connected but civically unprotected. Within the European context, disparities in cybersecurity curricula across higher education institutions reveal the lack of a regional policy vision. Salminen et al. (2023) found significant inconsistencies in course offerings, competencies, and institutional priorities, indicating that even within well-regulated regions like the EU, educational cybersecurity remains fragmented and underdeveloped. This policy incoherence extends to the **cybersecurity workforce pipeline**, which remains chronically undersupplied despite growing demand. Lewis and Crumpler (2019) describe this gap as a policy failure, arguing that governments have not invested in the necessary educational infrastructure to build resilient digital economies. Without integrated education-to-employment pathways, the shortfall in cybersecurity professionals persists, affecting not only industry but educational institutions themselves.

Another dimension of the policy gap is the disconnect between cybersecurity education and national defense strategies. While many nations have introduced defense-oriented cyber frameworks, these often operate in isolation from the education sector. Kumar et al. (2023) stress that without coordinated engagement between ministries of defense, education, and digital affairs, systemic vulnerabilities remain unaddressed. The absence of civic cybersecurity training in most national curricula exacerbates the exposure of students to digital risks. Limnell et al. (2023) argue that digital literacy alone is insufficient; students must be educated in digital ethics, privacy rights, and personal cybersecurity practices. The failure to embed such content into early education perpetuates ignorance and erodes digital citizenship. Even in higher education, policy gaps are evident in the failure to **integrate** regulatory compliance and data ethics into student training. García-Gómez (2022) notes that few institutions teach students

how to navigate the legal landscape of data protection, privacy, or cybersecurity compliance. As a result, graduates may enter the workforce with significant technical skills but little awareness of legal responsibilities or ethical considerations. The literature reveals an urgent need for policy harmonization and institutional reform to bridge cybersecurity and data protection gaps in education. Without cohesive frameworks and clearly articulated responsibilities, students remain vulnerable to cyber threats and privacy violations. The absence of national standards, funding support, and curricular mandates not only weakens institutional resilience but undermines the foundational principles of educational equity and student safety in digital environments.

Best Practices and Frameworks for Cybersecurity in Education

In response to escalating cyber threats in the education sector, a growing body of literature has advocated for the adoption of structured cybersecurity frameworks tailored to institutional needs. These frameworks offer strategic and technical guidance for securing educational environments, mitigating risks to student data, and ensuring long-term digital resilience. Best practices emerging from government, industry, and academic collaboration underscore the importance of standardized approaches, continual assessment, and cross-institutional alignment in creating robust cybersecurity ecosystems. One of the most widely adopted models in higher education is the integration of ISO/IEC 27001 and the NIST Cybersecurity Framework (NIST-CSF). These frameworks emphasize structured risk assessment, incident response planning, and policy-driven governance, enabling institutions to proactively manage vulnerabilities and safeguard student information systems (Bondoc & Malawit, 2020). By promoting security through layered controls, both standards support the implementation of technical safeguards such as encryption, access management, and audit trails.

The NICE Workforce Framework, developed by the U.S. National Institute of Standards and Technology, adds a workforce development lens to cybersecurity planning. It outlines specific knowledge, skills, and tasks (TKS) necessary for cybersecurity roles, allowing institutions to align their curricula with evolving workforce demands and security responsibilities (Petersen et al., 2020). This ensures that institutional capacity is not only technical but also human-centered. Building on NICE, the SPARTA Cybersecurity Skills Framework (CSF) introduces a European perspective, linking cybersecurity education directly to occupational roles through structured curricula design. This role-based model helps universities ensure that cybersecurity programs prepare graduates for real-world applications and regulatory environments (Hajny et al., 2021). It also bridges the gap between cybersecurity education and national employment strategies in digital security.

At the institutional level, a comprehensive cybersecurity strategy must encompass governance, risk management, stakeholder collaboration, and technical defense. Kumar et al. (2024) argue that effective frameworks should include not only technical protocols but also organizational structures that define roles, responsibilities, and reporting procedures in case of breaches. This holistic approach ensures alignment across IT, legal, academic, and administrative units. Collaborative efforts such as **EduCERT** offer an operational blueprint for higher education institutions to coordinate cyber incident response. This model facilitates cross-institutional information sharing, vulnerability disclosures, and national-level synchronization of education-sector cyber defenses (Otoom et al., 2024). It embodies a proactive approach to threat intelligence, enabling institutions to act collectively rather than in isolation. Other standards, such as ISO/IEC 27002, emphasize continuous improvement and policy alignment as essential to cybersecurity resilience. These practices support institutions in regularly updating risk assessments, testing incident response mechanisms, and embedding a culture of compliance and accountability (Amine et al., 2023). This adaptive capability is critical in light of rapidly evolving cyber threats and regulatory landscapes.

Pedagogical approaches to cybersecurity education also play a central role. Effective learning strategies include blended delivery models, simulation-based labs, and project-based curricula that build both technical competencies and contextual awareness (Mukherjee et al., 2024). These experiential formats deepen learner engagement and better prepare students for the complexity of real-world cybersecurity challenges. Frameworks such as CyBOK (Cyber Body of Knowledge) and CSEC2017 expand cybersecurity education by integrating core topics across computer science, human factors, ethics, and law. By fostering multidisciplinary fluency, these standards enable institutions to train cybersecurity professionals who are technically proficient and ethically grounded (Hajny et al., 2021). Emerging models emphasize agility and adaptability in cybersecurity frameworks. Petersen et al. (2020) stress that educational institutions must be equipped not only with technical tools but also with agile structures capable of evolving alongside new threats. Interoperability between systems, rapid feedback loops, and flexible governance are essential to long-term institutional resilience.

Finally, the COLTRANE framework brings a human-centered perspective to cybersecurity education. It incorporates soft skills such as communication, collaboration, and decision-making into cybersecurity training, recognizing that effective defense relies not only on technical knowledge but also on interpersonal and organizational dynamics (Langner et al., 2023). Best practices in cybersecurity for education require multi-layered strategies that integrate technical frameworks, human capacity development, pedagogical innovation, and governance coherence. While no single model is universally applicable, the convergence of standards such as NIST-CSF, ISO/IEC 27001, EduCERT, and CyBOK offers a blueprint for securing educational ecosystems against rising cyber threats. Institutions that proactively adopt, contextualize, and institutionalize these frameworks are better positioned to protect student data, ensure regulatory compliance, and foster trust in digital learning environments.

Conceptual Framework

The analysis of cybersecurity in online education reveals a complex ecosystem characterized by technical vulnerabilities, policy fragmentation, ethical tensions, and organizational disparities. In response, this study proposes the **Student-Centric Cybersecurity Governance Model (SCCGM)**—a conceptual framework that synthesizes threats, institutional responsibilities, and policy pathways to protect student digital identities. The SCCGM situates student privacy and security at the core of cybersecurity strategy, recognizing the learner not merely as a data subject but as a rights-bearing digital citizen. The model is anchored in four interlinked domains, each corresponding to a major theme identified in the literature: (1) **Threat Vectors and Systemic Vulnerabilities**, (2) **Privacy and Data Governance Ethics**, (3) **Policy and Regulatory Gaps**, and (4) **Cybersecurity Governance and Best Practices**. Each domain interacts with the others, illustrating that secure online education cannot be achieved through isolated technological fixes or standalone policies. Rather, it demands an integrated, student-centered approach that merges technical, legal, pedagogical, and ethical considerations.

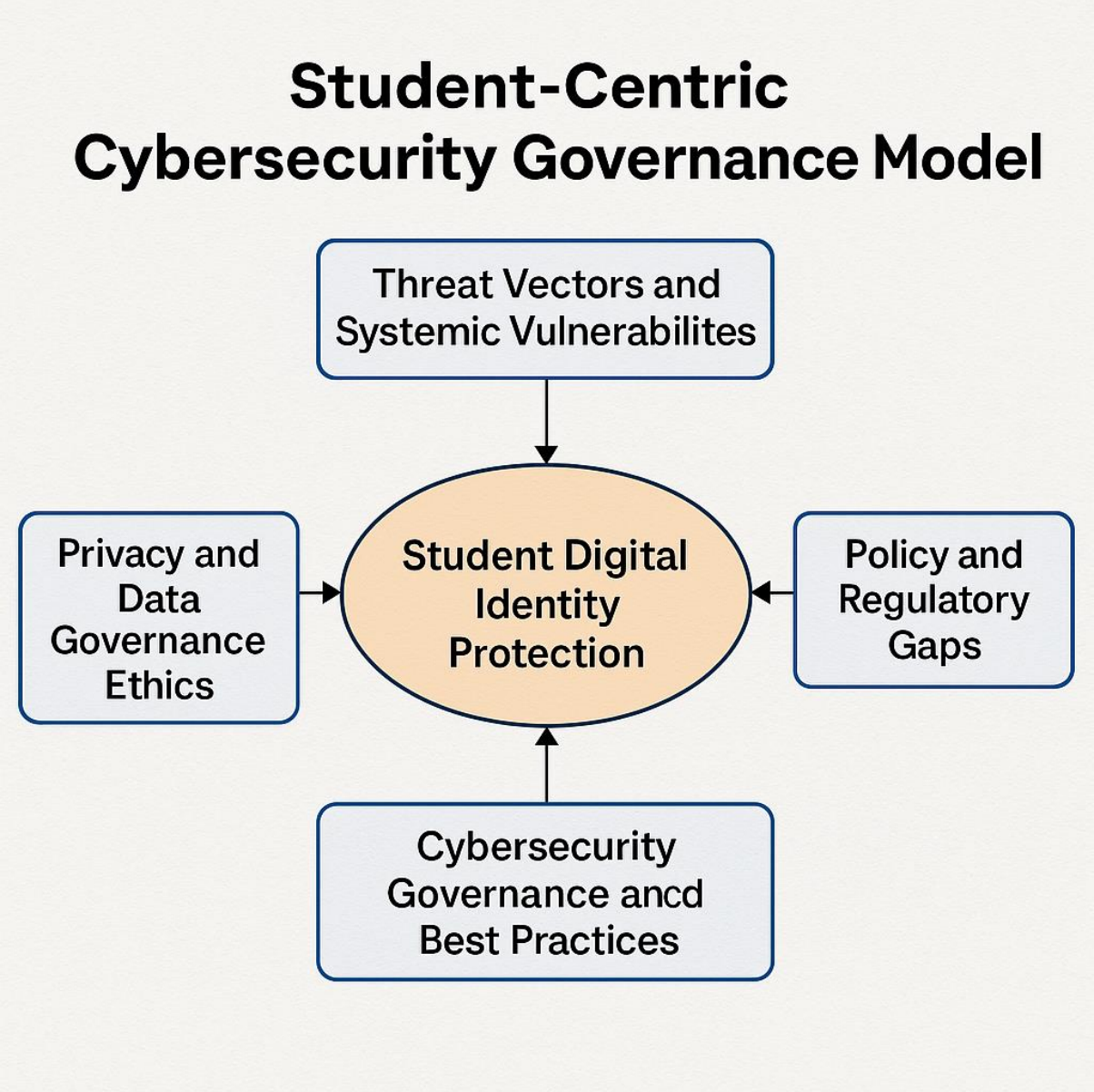

Figure 1: the **Student-Centric Cybersecurity Governance Model. Source: Authors' conceptualisation.**

The first domain—**Threat Vectors and Systemic Vulnerabilities**—captures the range of cybersecurity threats confronting educational institutions. These include ransomware, phishing, data breaches, and insider threats that exploit under-secured learning platforms and decentralized data infrastructures. Personal devices, remote desktops, and third-party applications amplify these risks, particularly in BYOD environments where security protocols are often uneven or absent (Sophos, 2024; Virtru, 2021). The model positions these vulnerabilities as the initial entry points that compromise digital identity integrity. The second domain—**Privacy and Data Governance Ethics**—frames the legal and ethical dilemmas that arise from the collection, storage, and analysis of student data. Legacy regulations such as FERPA and COPPA are shown to be insufficient for governing AI-enhanced, cloud-based learning environments, particularly in light of vendor opacity, biometric data use, and behavioral surveillance (Kelso et al., 2024; Chantal et al., 2023). The SCCGM thus calls for a redefinition of data governance principles that prioritize informed consent, transparency, and student agency.

The third domain—**Policy and Regulatory Gaps**—addresses the fragmentation of national and institutional policies. It reflects the mismatch between cybersecurity threats and the readiness of educational systems to counter them. Disparities in funding, inconsistent curricular mandates, and the absence of coordinated national frameworks have left many institutions exposed (Fouad, 2021; Lewis & Crumpler, 2019). This domain underscores the urgent need for harmonized policies that align digital citizenship, educational governance, and cybersecurity defense. The final domain—**Cybersecurity Governance and Best Practices**—integrates actionable frameworks such as ISO/IEC 27001, NIST-CSF, NICE, and EduCERT into educational contexts. These standards provide not only technical guidance but institutional structures for accountability, incident response, and compliance (Kumar et al., 2024; Bondoc & Malawit, 2020). The SCCGM emphasizes the importance of institutionalizing these frameworks through stakeholder training, policy enforcement, and cross-agency cooperation.

At the center of the SCCGM is the construct of **Student Digital Identity Protection**, which functions as both the normative goal and evaluative benchmark of the model. All four domains orbit and support this core objective. The framework conceptualizes digital identity protection not only as risk mitigation but as an ethical imperative tied to trust, autonomy, and equitable access to digital learning. In doing so, the SCCGM provides a policy-relevant, systems-level lens through which educational stakeholders can assess and improve cybersecurity resilience. Ultimately, the SCCGM reframes cybersecurity governance in education as a matter of **interconnected responsibilities**—technical, institutional, and regulatory. It highlights the need for cohesive action grounded in inclusive design, legal reform, student empowerment, and strategic foresight. As educational environments grow increasingly digitized, this framework serves as a guide for ensuring that digital transformation is not only innovative but just.

Methodology

This study employs a **qualitative conceptual methodology**, drawing upon **documentary research and thematic analysis** to construct the *Student-Centric Cybersecurity Governance Model (SCCGM)*. The approach is rooted in the need to critically examine fragmented cybersecurity practices and policy gaps within online education through the systematic synthesis of secondary data. Rather than testing predefined hypotheses, this study explores the complex, interrelated conditions shaping the governance of student digital identities. The research is based on an extensive corpus of literature, policy documents, technical standards, and institutional reports published between 2018 and 2025. Sources were purposively selected based on their relevance to four thematic areas: threat vectors and system vulnerabilities, privacy and data governance, policy frameworks in education, and best practices in cybersecurity. Authoritative materials from regulatory agencies (e.g., FTC, U.S. Department of Education), global institutions (e.g., UNESCO, NIST, ISO), academic journals, and EdTech policy consortia were prioritized to ensure credibility and policy relevance.

To guide the analysis, the study followed **Braun and Clarke's (2006) reflexive thematic analysis framework**. The process began with deep familiarization with the literature, followed by open coding of text segments to identify recurrent concepts, patterns, and concerns. Codes were then grouped into initial themes which were iteratively refined through constant comparison, ultimately resulting in four higher-order categories corresponding to the structure of the SCCGM. These themes did not emerge from frequency alone but from their theoretical centrality to understanding student digital identity protection. The development of the conceptual model was further shaped by **critical policy analysis**, emphasizing power asymmetries between educational institutions, EdTech vendors, and students. This orientation was particularly valuable in identifying how gaps in data governance and cybersecurity standards disproportionately expose marginalized learners. The model was also informed by

digital citizenship theory, which frames cybersecurity not merely as a technical or legal concern, but as a civic and ethical obligation tied to student autonomy, rights, and participation in online learning environments.

Source triangulation ensured robustness. Documents were drawn from multiple jurisdictions and institutional types—public schools, universities, regulatory agencies, and vendor platforms—to provide a diverse and comparative perspective. Triangulation across regulatory, technical, and pedagogical sources helped validate the thematic convergence that formed the backbone of the SCCGM. Moreover, interdisciplinary coherence was achieved by integrating insights from cybersecurity engineering, educational policy, information ethics, and critical digital studies. The absence of primary data is acknowledged as a limitation but also a deliberate methodological choice. Given the rapid pace of change in educational technology and the proliferation of publicly available policy material, documentary analysis offered a timely and ethically appropriate strategy for engaging with complex governance challenges without compromising privacy or institutional sensitivities.

This methodology supports the construction of a theoretically grounded, contextually relevant, and policy-actionable model. It reflects the study's core objective: to provide a strategic and normative framework for enhancing student-centered cybersecurity governance in digital education environments. By synthesizing global evidence through a critical, structured, and reflexive process, the SCCGM offers both diagnostic clarity and prescriptive potential.

Findings

The thematic synthesis of policy documents, regulatory frameworks, and scholarly literature revealed four interlocking domains that collectively inform the Student-Centric Cybersecurity Governance Model (SCCGM). Each domain reflects a distinct but interconnected dimension of student digital identity protection in online education. The findings highlight not only the diverse threat landscape confronting educational institutions, but also the institutional blind spots, policy inconsistencies, and governance challenges that contribute to student vulnerability in digital learning environments. The first domain, **Threat Vectors and Systemic Vulnerabilities**, captures the diverse cyber threats that target online education platforms. These include ransomware attacks, phishing campaigns, data breaches, and insider threats—each exploiting technological gaps and institutional complacency. Students are particularly at risk due to poor endpoint security in BYOD contexts, limited cyber hygiene education, and insecure integrations with third-party applications (Sophos, 2024; Virtru, 2021; LevelBlue, 2024). The proliferation of unregulated platforms, especially during the post-pandemic surge in remote learning, has further exacerbated the threat landscape.

The second domain, **Privacy and Data Governance Ethics**, reveals a lack of transparency and control in the ways student data is collected, stored, and shared. Legacy regulations such as FERPA and COPPA fall short in managing cloud-based systems, biometric surveillance, and learning analytics used in modern EdTech environments (ASCD, n.d.; Chantal et al., 2023). Consent practices are often perfunctory or entirely absent, leaving students unaware of how their data is being monetized or profiled. Ethical lapses around biometric data use and opaque third-party contracts emerged as critical concerns. The third domain, **Policy and Regulatory Gaps**, exposes fragmented national and institutional approaches to cybersecurity and digital governance in education. While the U.S. and EU have introduced overarching privacy laws, they often fail to account for the specific risks and needs of educational settings (Sun, 2023; Salminen et al., 2023). Policy misalignment across ministries, funding shortfalls, and the lack of national cybersecurity curricula have left institutions underprepared. The education sector's peripheral engagement in broader national cyber defense strategies further compounds institutional vulnerability (Fouad, 2021; Lewis & Crumpler, 2019).

The fourth domain, **Cybersecurity Governance and Best Practices**, illustrates the strategic potential of adopting internationally recognized frameworks such as NIST-CSF, ISO/IEC 27001, NICE, and EduCERT. These models offer roadmaps for structured risk management, workforce training, and incident response. However, their uptake in educational settings remains inconsistent, often hindered by a lack of institutional capacity or awareness (Bondoc & Malawit, 2020; Kumar et al., 2024). Where applied effectively, these frameworks enhance accountability and provide sustainable security infrastructure aligned with evolving threats. Together, these findings support the SCCGM's central proposition: that safeguarding student digital identities requires a multi-dimensional governance strategy grounded in inclusivity, transparency, and regulatory alignment. By identifying the interactions between threat exposure, ethical oversight, policy coherence, and best-practice implementation, the model offers a comprehensive framework for institutional and systemic cybersecurity enhancement in online education.

SCCGM Domain	Key Insights	Representative Sources
Threat Vectors and Systemic Vulnerabilities	Students face ransomware, phishing, insider threats, and poor device security in online education.	Sophos (2024); Virtru (2021); LevelBlue (2024)
Privacy and Data Governance Ethics	Data is collected with minimal transparency; biometric tracking and analytics lack informed consent.	ASCD (n.d.); Chantal et al. (2023); Kelso et al. (2024)
Policy and Regulatory Gaps	National frameworks are inconsistent; FERPA, GDPR lack educational specificity and enforcement.	Sun (2023); Fouad (2021); Salminen et al. (2023)
Cybersecurity Governance and Best Practices	ISO, NIST, NICE, EduCERT frameworks offer scalable governance but are underutilized in education.	Bondoc & Malawit (2020); Kumar et al. (2024)

Discussion

The findings of this study emphasize the urgent need to reconceptualize cybersecurity in education as an issue of **systemic governance** rather than isolated technical intervention. The Student-Centric Cybersecurity Governance Model (SCCGM) highlights the convergence of threat escalation, ethical oversight failures, policy incoherence, and underutilized best practices, all of which contribute to student vulnerability in increasingly digitized learning environments. As education systems worldwide expand their dependence on AI-driven tools and cloud-based infrastructure, the importance of a coordinated, student-first approach to cybersecurity becomes not only practical but ethically imperative. The first dimension of the SCCGM—**Threat Vectors and Systemic Vulnerabilities**—reveals how institutions remain exposed to basic and advanced cyberattacks due to architectural weaknesses and operational oversight. The escalation in ransomware and phishing attacks shows that the education sector is no longer a peripheral target but a primary one for threat actors (Sophos, 2024; Prey Project, 2024). While the private sector has broadly adopted endpoint protection, zero-trust models, and real-time intrusion monitoring, many schools and universities lag behind due to resource constraints, BYOD policies, and a fragmented approach to IT governance (Virtru, 2021; LevelBlue, 2024). This vulnerability is compounded by a lack of cyber hygiene education, particularly among students, who often unknowingly function as the weakest links in digital security ecosystems.

The second domain—**Privacy and Data Governance Ethics**—brings to light the deeper crisis of legitimacy that current governance models face. Regulatory frameworks like FERPA and COPPA were designed in pre-cloud, pre-AI eras, and their outdated provisions do not adequately address data sharing with third-party vendors, biometric tracking, or behavioral analytics embedded in EdTech platforms (ASCD, n.d.; Chantal et al., 2023). In many cases, data is collected without genuine consent, processed without transparency, and monetized without oversight. These practices not only violate students' digital autonomy but also contribute to a chilling effect on learning, as constant surveillance discourages exploration and dissent (Kelso et al., 2024; Mutimukwe et al., 2021). Crucially, the findings demonstrate that **students are rarely treated as data subjects with enforceable rights**. The normalization of surveillance tools such as keystroke monitors and facial recognition, often justified under the guise of safety or academic integrity, has led to widespread ethical concerns. This aligns with critical digital ethics literature that argues for a reframing of educational data governance through principles of fairness, explainability, and proportionality (New America, 2024). Without strong ethical foundations, even technically secure systems can reproduce injustice and erode trust.

The third domain—**Policy and Regulatory Gaps**—further underscores the uneven terrain of cybersecurity preparedness. While some regions have adopted forward-looking policies, such as the GDPR in Europe or national cybersecurity standards in select U.S. states, these efforts remain inconsistent and poorly aligned with educational realities (Sun, 2023; Salminen et al., 2023). Many institutions continue to treat cybersecurity as a reactive function rather than a strategic imperative, with minimal integration into leadership, curriculum, or professional development. This reflects what Fouad (2021) terms a "structural marginalization of cybersecurity" in higher education governance. The absence of national cybersecurity curricula—particularly in K–12 education—is perhaps the most significant policy failure. Without mandated instruction in digital citizenship, privacy, and risk mitigation, students are left ill-equipped to navigate the complex terrain of online threats (Limnell et al., 2023). This educational gap not only places learners at risk but weakens the broader societal effort to cultivate a cyber-resilient population capable of defending democratic and institutional integrity in a digital age.

Finally, the fourth domain—**Cybersecurity Governance and Best Practices**—offers a path forward. The findings show that while globally validated frameworks such as NIST-CSF, ISO/IEC 27001, and EduCERT exist, they are not widely embedded in education-sector governance (Bondoc & Malawit, 2020; Kumar et al., 2024). Where these models have been adopted, institutions benefit from structured risk management, incident response planning, and compliance auditing. However, integration remains sporadic, often depending on the presence of cybersecurity leadership or participation in national grant initiatives. The SCCGM model brings these threads together by placing **student digital identity protection** at the center of cybersecurity governance. It challenges institutions to move beyond minimal compliance toward proactive engagement with ethical, technical, and pedagogical dimensions of digital security. Student-centered cybersecurity reframes risk not only in terms of breach prevention, but in terms of rights preservation, trust-building, and institutional legitimacy.

The implications for policymakers are profound. First, cybersecurity must be integrated into national education strategies—not as an add-on, but as a foundational competency. Second, legislation must be updated to reflect the realities of cloud computing, behavioral analytics, and cross-border data flows in education. Third, public-private partnerships with EdTech vendors must be governed by clear contractual obligations around data minimization, anonymization, and breach disclosure. For educational leaders, the SCCGM encourages the institutionalization of cybersecurity training across faculty, staff, and students; the adoption of flexible, scalable frameworks; and the inclusion of digital ethics in curriculum design. Only

through such multidimensional efforts can educational institutions evolve into digitally resilient, rights-respecting learning environments. Cybersecurity in education is no longer a technical afterthought—it is a **governance imperative**. The SCCGM provides a roadmap for aligning technical innovation with student protection, policy reform, and ethical accountability. As online education becomes ubiquitous, the ability of institutions to secure and respect digital identities will define not only their legitimacy but their very mission in the digital age.

Conclusion

This study has illuminated the multi-layered cybersecurity challenges inherent in online education, particularly as they relate to the protection of student digital identities. Drawing upon a comprehensive review of recent literature and policy documents, it developed the *Student-Centric Cybersecurity Governance Model (SCCGM)* to conceptualize a rights-based and systemic approach to digital security in educational environments. The findings reinforce that the risks facing students—ranging from ransomware and phishing to invasive surveillance and weak regulatory protections—are not merely technical flaws but manifestations of broader governance deficits. The SCCGM framework positions student data privacy and security as ethical imperatives that must be embedded across institutional operations, technology integration, and national education policies. It offers a structured yet flexible roadmap that links threat identification, data governance, policy coherence, and best-practice frameworks into a unified governance architecture. Rather than treating cybersecurity as an IT function or reactive defense, this model foregrounds it as a core component of educational integrity, student agency, and democratic participation in the digital age. As the global shift to online and hybrid learning accelerates, institutions and governments must move decisively to protect learners from the growing spectrum of digital harms that threaten both their academic and personal futures.

Recommendations

To actualize the principles embedded in the SCCGM, educational institutions must adopt a more proactive and integrated approach to cybersecurity governance. Institutional leaders should prioritize the development of internal cybersecurity policies that reflect current threat landscapes and student protection mandates. These policies should be shaped in consultation with legal, pedagogical, and technical stakeholders, ensuring that data privacy and digital identity protection are not siloed concerns but organization-wide priorities. Governments must revise and harmonize national privacy and education laws to address the realities of AI-driven learning, biometric surveillance, and vendor-driven data ecosystems. Existing frameworks like FERPA and COPPA must be modernized to include explicit provisions for consent, data portability, breach transparency, and biometric protections. Simultaneously, governments should support the development and funding of cybersecurity education from K–12 through higher education, embedding digital citizenship and ethics into national curricula. At the vendor level, EdTech companies must be held to higher accountability standards, with enforceable contracts that define data ownership, access limitations, and ethical design expectations. Transparency audits and third-party compliance verification should become standard regulatory practices for any technology deployed in educational contexts. Public-private partnerships must be grounded in public interest safeguards, not solely efficiency or cost-effectiveness. Finally, cross-agency and international collaboration must be strengthened. Just as cyber threats transcend institutional and national boundaries, so too must the responses. Education ministries, data protection authorities, civil society, and international regulatory bodies should work toward interoperable standards and joint enforcement mechanisms. Through such multi-level, student-centered governance, the promise of digital education can be realized without sacrificing the rights, security, and dignity of the learners it seeks to serve.

References

Amine, A. M., Chakir, E. M., Issam, T., & Idrissi Khamlichi, Y. (2023). A review of cybersecurity management standards applied in higher education institutions. *International Journal of Safety and Security Engineering*, 13(6), 635–645. https://doi.org/10.18280/ijsse.130614

AP News. (2023, December 20). *FTC proposes strengthening children's online privacy rules to address tracking, push notifications*. Retrieved from https://apnews.com/article/352ba63293832ee930f0c137aac735de

ASCD. (n.d.). *The Challenge of Data Privacy*. Retrieved from https://www.ascd.org/el/articles/the-challenge-of-data-privacy

Bondoc, C. E., & Malawit, T. G. (2020). Cybersecurity for higher education institutions: Adopting regulatory framework. *Global Journal of Engineering and Technology Advances*, 2(3), 99–108. https://doi.org/10.30574/GJETA.2020.2.3.0013

Chantal, M., Shengnan, H., Viberg, O., & Cerratto-Pargman, T. (2023). *Privacy as Contextual Integrity in Online Proctoring Systems in Higher Education: A Scoping Review*. arXiv preprint arXiv:2310.18792. https://arxiv.org/abs/2310.18792

Crabb, J., Hundhausen, C., & Gebremedhin, A. H. (2024). A critical review of cybersecurity education in the United States. *Proceedings of the ACM Technical Symposium on Computer Science Education*, 1–9. https://doi.org/10.1145/3626252.3630757

EdTech Magazine. (2024, April). *Data Governance Policies Are a Must for Schools*. Retrieved from https://edtechmagazine.com/k12/article/2024/4/data-governance-in-schools-perfcon

EdTech Magazine. (2024, November 15). *Remote Desktops Pose Security Risks for Online Learners*. https://edtechmagazine.com/higher/article/2024/11/remote-desktops-pose-security-risks-online-learners

Fouad, N. S. (2021). Securing higher education against cyberthreats: From an institutional risk to a national policy challenge. *Journal of Cyber Policy*, *6*(1), 30–47. https://doi.org/10.1080/23738871.2021.1973526

García-Gómez, S. (2022). Cyber security threats to educational institutes: A growing concern for the new era of cybersecurity. *Preprints*. https://doi.org/10.20944/preprints202211.0128.v1

Hajny, J., Ricci, S., Piesarskas, E., Levillain, O., Galletta, L., & De Nicola, R. (2021). Framework, tools and good practices for cybersecurity curricula. *IEEE Access*, 9, 98307–98319. https://doi.org/10.1109/ACCESS.2021.3093952

Johns Hopkins University. (2024, August 20). *Unseen Dangers Lurking in Storing Student Data in the Cloud*. https://ep.jhu.edu/news/cloudy-with-a-chance-of-breach-unseen-dangers-lurking-in-storing-student-data-in-the-cloud/

Kelso, E., Soneji, A., Rahaman, S., Soshitaishvili, Y., & Hasan, R. (2024). *Trust, Because You Can't Verify: Privacy and Security Hurdles in Education Technology Acquisition Practices*. arXiv preprint arXiv:2405.11712. https://arxiv.org/abs/2405.11712

Kumar, A., Mishra, K., Mahto, R. K., & Mishra, B. K. (2024). A framework for institution to enhancing cybersecurity in higher education: A review. *LATIA Journal*, 1(1), 10–23. https://doi.org/10.62486/latia202494

Kumar, G. E. P., Pandey, S. K., Varshney, N., Kumar, A., & Singh, K. U. (2023). Cybersecurity education: Understanding the knowledge gaps based on cybersecurity policy, challenge, and knowledge. *Proceedings of the International Conference on Communication Systems and Network Technologies, 2023*, 445–451. https://doi.org/10.1109/CSNT57126.2023.10134610

Langner, G., Furnell, S., Quirchmayr, G., & Skopik, F. (2023). A comprehensive design framework for multi-disciplinary cybersecurity education. In *Foundations of*

Information Security Education (pp. 117–132). Springer. https://doi.org/10.1007/978-3-031-38530-8_9

LevelBlue. (2024, September 5). *Enhancing Cybersecurity in Online Learning*. https://levelblue.com/blogs/security-essentials/tackling-the-unique-cybersecurity-challenges-of-online-learning-platforms

Lewis, J. A., & Crumpler, W. (2019). The cybersecurity workforce gap. *Center for Strategic and International Studies*. https://scispace.com/papers/the-cybersecurity-workforce-gap-vjim7twfe4

Limnell, E., Salminen, M., Cullen, K., Latvanen, S., & Matilainen, T. (2023). Cybersecurity education in European higher education institutions. *Proceedings of the International Conference on Higher Education Advances*, *3*(1), 125–138. https://doi.org/10.4995/head23.2023.16336

Malecki, A. (2018). Cybersecurity in the classroom: Bridging the gap between computer access and online safety. *Education and Information Technologies*, *23*(4), 1731–1745. https://scispace.com/papers/cybersecurity-in-the-classroom-bridging-the-gap-between-2erfiqkiwr

Mukherjee, M., Le, N., Chow, Y. W., & Susilo, W. (2024). Strategic approaches to cybersecurity learning: A study of educational models and outcomes. *Information*, 15(2), 117. https://doi.org/10.3390/info15020117

Mutimukwe, C., Twizeyimana, J. D., & Viberg, O. (2021). *Students' Information Privacy Concerns in Learning Analytics: Towards a Model Development*. arXiv preprint arXiv:2109.00068. https://arxiv.org/abs/2109.00068

MySanAntonio. (2025, February 8). *Almost 800K Texans impacted by school software data breach*. https://www.mysanantonio.com/business/article/powerschool-data-breach-20153556.php

NASBE. (n.d.). *Ensuring Student Data Privacy through Better Governance*. Retrieved from https://www.nasbe.org/ensuring-student-data-privacy-through-better-governance/

New America. (2024, December). *Empowering Student Agency in the Digital Age: The Role of Privacy in EdTech*. Retrieved from https://www.newamerica.org/education-policy/briefs/empowering-student-agency-in-the-digital-age-the-role-of-privacy-in-edtech/

Otoom, A., Atoum, I., Al-Harahsheh, H., Aljawarneh, M., Al Refai, M. N., & Baklizi, M. (2024). A collaborative cybersecurity framework for higher education. *Information & Computer Security*, Advance online publication. https://doi.org/10.1108/ICS-02-2024-0048

Petersen, R., Santos, D., Smith, M. C., & Witte, G. A. (2020). Workforce framework for cybersecurity (NICE framework). *NIST Special Publication 800-181 Revision 1*. https://doi.org/10.6028/NIST.SP.800-181r1

Prey Project. (2024, March 15). *School phishing: essential tips to win the battle*. https://preyproject.com/blog/school-phishing-and-ransomware

Salminen, M., Cullen, K., Latvanen, S., & Matilainen, T. (2023). Cybersecurity education in European higher education institutions. *Proceedings of the International Conference on Higher Education Advances*, *3*(1), 125–138. https://doi.org/10.4995/head23.2023.16336

Sophos. (2024, July 11). *The State of Ransomware in Education 2024*. https://news.sophos.com/en-us/2024/07/11/the-state-of-ransomware-in-education-2024/

Student Privacy Compass. (n.d.). *Data Security: K-12 and Higher Education*. https://studentprivacy.ed.gov/data-security-k-12-and-higher-education

Sun, J. C. (2023). Gaps, guesswork, and ghosts lurking in technology integration: Laws and policies applicable to student privacy. *British Journal of Educational Technology*, *54*(5), 1083–1100. https://doi.org/10.1111/bjet.13379

The 74. (2025, February 4). *Meet the Hired Guns Who Make Sure School Cyberattacks Stay Hidden*. https://www.wired.com/story/meet-the-hired-guns-who-make-sure-school-cyberattacks-stay-hidden

U.S. Department of Education. (2014, February). *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices*. Retrieved from https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29_0.pdf

Virtru. (2021, March 15). *Cybersecurity Risks in eLearning*. https://www.virtru.com/blog/data-centric-security/education/elearning

Watini, S., Davies, G., & Andersen, N. (2024). Cybersecurity in learning systems: Data protection and privacy in educational information systems and digital learning environments. *Information Technology and Education*, *3*(1), 55–69. https://doi.org/10.33050/itee.v3i1.665

Western Governors University. (2024, November 10). *Cybersecurity Awareness for Online Learners: Protecting Your Digital Identity*. https://www.wgu.edu/blog/cybersecurity-awareness-online-learners-protecting-your-digital-identity2407.html

Wikipedia. (n.d.). *Student monitoring software*. Retrieved from https://en.wikipedia.org/wiki/Student_monitoring_software