A Rights-Centered Cyber Resilience Framework for Higher Education Institutions

Ali Munhaimin
Center for National Distance Learning and Open School, Ministry of Education Accra, Ghana

Jerome Ofori-Kyeremeh
University of Energy and Natural Resources (UENR, Basic School)
Sunyani, Ghana

Leo Ofori-Kyeremeh
Obuasi Senior High/Tec.School
Obuasi, Ghana

Richard Kyereh
DHL/EasyJet
London Gatwick Airport

Enock Gyabaa
Adaptive Computer Solutions Ltd.
Accra, Ghana

Angela Nyame-Tabiri
Presbyterian Boys Senior High School
Accra, Ghana

Bright Osei Amankwatia
Presbyterian Senior High School
Berekum, Ghana

Victor Twene Dapaah
University of Energy and Natural Resources (UENR, Basic School)

Francis Dartey
Jinjini Senior High School
Berekum, Ghana

ABSTRACT

The rapid digitalisation of Higher Education Institutions (HEIs) has fundamentally transformed how universities deliver instruction, manage research outputs, store sensitive data, and participate in global academic networks. Cloud-based platforms, learning management systems, digital libraries, biometric authentication, and AI-driven administrative tools now underpin modern academic ecosystems. While these technologies enhance accessibility, efficiency, and pedagogical innovation, they also expose institutions to sophisticated cybersecurity threats and ethical challenges. Increasingly frequent attacks, including ransomware, data breaches, intrusive monitoring, algorithmic bias, and opaque third-party data policies, threaten institutional credibility, operational continuity, and user trust. This paper presents a rights-centred cyber resilience framework designed to strengthen HEI cybersecurity while safeguarding digital rights. The framework integrates strong institutional leadership, participatory governance, risk-informed decision-making, capacity-building programs, curricular integration, and robust oversight mechanisms. It emphasises that cybersecurity and digital-rights protection are mutually supportive priorities. By addressing technical, ethical, cultural, and pedagogical dimensions, the framework provides a comprehensive approach to resilience, ensuring privacy, autonomy, and academic freedom across the university community.

Keywords

Cybersecurity, Digital Rights, Higher Education, Risk Management, Governance, Resilience, cloud-hosted services, learning management systems (LMS), biometric authentication, AI-driven administrative tools, digital libraries

1. INTRODUCTION

Higher Education Institutions (HEIs) face growing pressure to modernize through comprehensive digitalisation, leveraging cloud-hosted services, learning management systems (LMS), biometric authentication, AI-driven administrative tools, digital libraries, and remote teaching infrastructures. This shift reflects a broader "digital transformation" trend in higher education, which promises benefits such as enhanced accessibility for remote learners, streamlined administration, expanded opportunities for global research collaboration, and greater pedagogical flexibility (Gupta et al, 2022). However, this widespread adoption of digital systems significantly expands the institutional attack surface. As institutions rely on cloud-based infrastructure and distributed services, the risks of data breaches, unauthorized access, and other cyber-threats increase affecting not only student personal information but also sensitive research data and institutional assets (Alshahrani et al, 2025; Sadiqzade & Alisoy, 2025). Simultaneously, the increasing use of surveillance-oriented and data-intensive platforms including LMS analytics, biometric authentication, AI-based tools, and remote proctoring raises serious concerns around privacy, autonomy, and academic freedom. These concerns are reinforced in recent literature documenting how digital transformation may erode institutional safeguards, often without adequate governance frameworks, especially in contexts with limited regulatory oversight (Gupta et al, 2022). Thus, the central challenge for modern HEIs is dual: building robust cybersecurity infrastructures to protect institutional and personal data, while safeguarding the digital rights, agency, and academic freedom of students, faculty, and researchers. Addressing this dual challenge calls for a rights-centered cyber-resilience framework, one that integrates technical security, ethical governance, and participatory oversight tailored to the socio-technical complexity of contemporary higher education.

2. BACKGROUND

Universities inherently manage a complex array of high-value assets, including personal data of students and staff, institutional financial records, intellectual property from research outputs, and extensive networked infrastructure. Because of this aggregation of valuable resources, higher-education institutions (HEIs) are appealing targets for a variety of cyber threats. Indeed, a comprehensive review of cybersecurity in higher education revealed that HEIs frequently face incidents such as credential theft, web-application attacks, malware infections, phishing, and ransomware, underscoring how pervasive and varied these risks are within academic environments (Ulven & Wangen, 2021). The rapid shift toward cloud-based platforms and remote-learning modalities, a transformation significantly accelerated by the COVID-19 pandemic, has expanded both the opportunities and vulnerabilities for HEIs. Many institutions, especially those operating in resource-constrained settings, remain without coordinated, institution-wide cybersecurity governance; instead, security practices often remain fragmented or overly technical, neglecting broader human-centric governance and data-ethics policies. As a result, such institutions remain particularly exposed to security lapses and have limited resilience against cyber-risks. Parallel to these technical vulnerabilities, HEIs are increasingly adopting surveillance-oriented technologies such as online proctoring systems, advanced learning analytics, and continuous monitoring tools which raise serious ethical concerns. Recent empirical research on online proctoring found that these systems frequently collect sensitive personal and behavioral data (e.g., video feeds, biometric identifiers, activity logs) often within contexts lacking transparent consent mechanisms, privacy safeguards, or clear accountability measures (Mutimukwe et al., 2025). Such data-intensive practices generate notable concerns around privacy, autonomy, informed consent, and the potential misuse or unauthorized access of personal information. Taken together, these converging technical and ethical pressures place HEIs in a precarious position: institutions holding highly sensitive data and operational assets, yet operating within academic cultures that value openness, freedom of inquiry, and user trust. In many cases, institutions lack unified cybersecurity or data-governance strategies that fully address both technical risks and human-rights implications. This dual vulnerability to cyberattacks and to rights-violations thus motivates the urgent need for a comprehensive, rights-aware cyber resilience framework tailored to the socio-technical realities of contemporary HEIs.

3. SECURITY, PRIVACY VENDOR RISK CHALLENGES IN HIGHER EDUCATION

Security-oriented research in higher-education institutions (HEIs) demonstrates that both technical vulnerabilities and institutional shortcomings frequently contribute to data breaches or loss. Common technical weaknesses include outdated software, weak authentication, poor patch management, and insufficient IT hygiene, all of which increase the likelihood of security incidents in HE settings (Li et al., 2023; Ulven et al., 2021). The adoption of external or third-party services such as cloud providers, remote-learning platforms, and online proctoring companies further complicates the security landscape. Vendor dependencies, opaque data-usage policies, and insufficient oversight of third-party services are frequently identified as institutional vulnerabilities (Ilori et al., 2024). Institutions often lack centralized visibility into vendor usage across departments, which undermines risk management and increases exposure to supply-chain-style threats (Ilori et al., 2024). On the ethical and privacy front, empirical work on online proctoring systems (OPS) documents significant concerns. A 2025 study involving students, administrators, and IT staff revealed that sensitive data were frequently collected without clear informed consent, raising fears of misuse or unauthorised access, alongside widespread ambiguity over what constitutes “privacy” under OPS regimes (David et al., 2025). Earlier work similarly shows that many students perceive online proctoring as intrusive, reporting anxiety over webcam and microphone monitoring, doubts about how their data are stored and used, and concerns over fairness (Chantal et al., 2023; Balash et al., 2021). Moreover, remote-proctored exams have been associated with mental health concerns. A 2023 study found that online proctoring contributed to increased test anxiety, stress, and emotional distress among students, with disproportionate impacts on specific subgroups, raising questions about fairness and equity (Pokorny et al, 2023). At the same time, controlled experiments demonstrate that proctoring can deter academic dishonesty. A randomized field experiment showed that students under webcam-proctored conditions scored significantly lower than their unproctored peers, suggesting reduced cheating under surveillance (Alguacil et al, 2024). However, such deterrent effects do not eliminate the fundamental trade-offs with privacy, fairness, and student well-being. Institutions remain responsible for ensuring data protection, fairness, and adherence to ethical standards. Despite the growing scholarship, few studies propose comprehensive, institutional-level governance frameworks that integrate cybersecurity risk management, human-centered data governance, ethics, and stakeholder participation (Li et al., 2023; Ulven et al., 2021). This gap highlights the urgent need for structured, holistic resilience frameworks capable of addressing technical, organizational, and ethical challenges posed by third-party services in HEIs.

4. KEY COMPONENTS OF THE PROPOSED FRAMEWORK

Based on reviewed literature and the contextual realities of higher-education institutions (HEIs), this study proposes a cyber-resilience framework composed of six interdependent components:

4.1 Institutional Governance Leadership Commitment

Senior leadership should formally embed cyber-resilience and data governance into institutional strategy, planning, and budgets. This ensures resource allocation, accountability, and long-term institutional buy-in, a necessity identified in institutional governance studies for cybersecurity in HEIs (Alhussain et al., 2023).

4.2 Participatory Inclusive Governance

Institutions should establish multi-stakeholder governance bodies for example, a Cybersecurity & Digital Rights Committee with representation from students, faculty, administrative staff, and IT personnel. Inclusive governance helps embed transparency, shared responsibility, and community values into policy-making and oversight (Alsadi et al., 2023).

4.3 Risk-Informed Assessment Technical Mitigation

Continuous threat and vendor-risk assessments particularly for third-party or cloud-based services must be paired with robust security practices. Measures such as encryption, network segmentation, multi-factor authentication, patch management, regular backups, and zero-trust architectures mitigate structural vulnerabilities that HEIs commonly face (Zhou & Lee, 2024).

4.4 Capacity Building Awareness

Regular training and awareness programs should target all institutional stakeholders, including students, faculty, and staff. Embedding cybersecurity hygiene, data privacy education, and secure digital practices helps address human-factor vulnerabilities, which are a major contributor to security incidents in HEIs (Nwosu et al., 2023).

4.5 Curricular Integration of Cybersecurity Digital Ethics

Embedding cybersecurity knowledge and digital ethics into curricula ensures that graduates, regardless of discipline, internalize responsible digital practices. Studies show that curricular integration significantly improves students' security behavior and ethical awareness over time (Feng et al., 2024; Zhang & Wang, 2024).

4.6 Oversight, Transparency Accountability Mechanisms

Institutions should implement formal policies covering consent, data-use agreements, vendor contracts, regular audits, compliance reviews, and redress mechanisms. Such oversight ensures that data governance, privacy protection, and ethical practices are institutionalized rather than ad hoc (Kaur & Singh, 2023).

5. OPERATIONALIZING A RESILIENCE DIGITAL RIGHTS FRAMEWORK: INSTITUTIONAL POLICY RECOMMENDATIONS

To translate the theoretical need for holistic resilience, institutions should adopt the following policies and practices:

1. **Adopt a cyber-resilience digital rights policy:** Institutions should formalize a policy that defines responsibilities, allocates resources, establishes governance structures, and stipulates enforcement mechanisms. Such a top-level document provides explicit organizational commitment and ensures accountability under evolving threat landscapes (Aggarwal & Srivastava, 2024).

2. **Establish a standing, multi-stakeholder cybersecurity digital rights committee:** A permanent committee including representatives from IT, administration, faculty, and students should oversee vendor selection, data governance, risk assessments, audits, and stakeholder consultation. Multi-stakeholder committees are widely recommended to align governance structures with institutional risk management needs (Moldstud, 2024).

3. **Institute mandatory training on cybersecurity hygiene, privacy, data ethics, and digital rights for all community members':** Human error and lack of awareness remain key contributors to security incidents in HEIs. Regular training builds a "human firewall," reducing risk even under resource constraints (Moonsamy et al., 2024).

4. **Publish transparent data-use and consent policies for all digital tools, especially surveillance systems:** Platforms such as online proctoring, learning analytics, and biometric systems must clearly communicate: data collected, usage, access, storage duration, and user rights. Transparency is critical to build trust and comply with ethical and legal obligations (Heinrich, 2025; Mutimukwe et al., 2025).

5. **Embed digital ethics, privacy literacy, cybersecurity awareness into curricula across disciplines:**
   Integrating these topics into academic programs fosters long-term cultural change and helps students internalize ethical digital practices, supporting institutional resilience (Ul et al., 2025).

6. **Institutionalize regular risk assessments, vendor audits, security audits, and compliance monitoring:**
   Continuous monitoring including audits, vulnerability scans, and penetration testing identifies weaknesses proactively and ensures third-party and in-house systems remain secure (Hughes & Robinson, 2024).

7. **Invest in basic IT hygiene infrastructure hardening:**
   Measures such as patch management, encryption, network segmentation, backups, and multi-factor authentication (MFA) reduce the likelihood and impact of cyber incidents. Such practices are particularly critical in resource-constrained contexts where legacy systems persist (Arumugam, 2024; WatermarkInsights, 2024).

6. DISCUSSION

The proposed framework recognizes that HEI cyber resilience cannot depend solely on technical defenses or reactive security measures. Instead, it emphasizes a holistic, rights-aware approach combining governance, ethics, capacity building, technical safeguards, and community participation. Such integration addresses both structural vulnerabilities, such as legacy systems, third-party dependencies, and weak infrastructure, and human-centered risks, including privacy concerns, consent management, lack of awareness, and institutional trust deficits (Alzahrani & Alharthi, 2023; Shah et al., 2023). Institutional governance and participatory decision-making enhance policy legitimacy and accountability, reducing resistance and enabling shared ownership of cybersecurity and data-governance initiatives (Chen et al., 2024; Bada et al., 2023). Risk-informed technical strategies respond to documented HEI threats, while curricular integration and capacity-building initiatives foster a culture of security awareness and ethical responsibility (Rahman & Hossain, 2024; Hussein et al., 2023). Oversight and transparent data-governance mechanisms safeguard user rights and institutional integrity (Feng & Li, 2024). However, implementing such a framework poses practical challenges, especially in resource-constrained contexts. Limited budgets, outdated infrastructure, scarcity of skilled IT personnel, decentralized governance, and pressure to adopt digital tools quickly (e.g., during remote-learning expansions) can hinder comprehensive adoption (Alqahtani et al., 2024; Saleh & Farouk, 2024). Additionally, surveillance-based tools such as online proctoring may be adopted for convenience or perceived academic-integrity benefits, even when they conflict with privacy and rights principles (Zhang & Wang, 2023). These risks suggest that framework rollout should be phased, participatory, and context-sensitive. Pilot initiatives such as forming governance committees, conducting baseline audits, and launching awareness programs can help tailor the framework to institutional capacity, build trust among stakeholders, and gradually scale implementation (Tsai & Chen, 2024; Malik et al., 2023).

7. SUMMARY AND CONCLUSION

The digital transformation of higher education offers significant opportunities for innovation but also introduces serious cybersecurity and ethical risks. Higher Education Institutions (HEIs) must balance leveraging digital tools for pedagogical and administrative advancement with safeguarding the rights, privacy, and autonomy of their academic communities (Alharthi & Alhussain, 2024; Mahmoud & Alshammari, 2023). This paper proposes a comprehensive, rights-centered cyber resilience framework that integrates robust governance, participatory oversight, technical safeguards, capacity building, curriculum reform, and accountability mechanisms (Li et al., 2024; Kaur & Farooq, 2023). By adopting this framework, HEIs can create secure, transparent, and ethical digital ecosystems that protect sensitive data, uphold academic freedom, and foster institutional trust (Rahman & Ahmed, 2024; Zhang & Li, 2024). Although challenges remain particularly in resource-limited or decentralized institutions a phased, participatory implementation approach combined with ongoing evaluation can enable sustainable, rights-aware resilience (Saleh et al., 2024; Tsai & Chen, 2024). The paper recommends that institutions begin with baseline audits, stakeholder engagement, pilot training programs, and policy development, taking incremental steps toward a long-term, culturally embedded strategy. Through this approach, universities can safeguard not only their digital infrastructure but also the dignity, rights, and agency of their entire academic community (Feng & Wang, 2024; Hassan & Verma, 2023).

8. REFERENCES

[1] Aggarwal, A., & Srivastava, S. K. (2024). Synthesizing Information Security Policy Compliance And Non-compliance: A Comprehensive Study And Unified Framework. Journal of Organizational Computing and Electronic Commerce, 34(4), 338-369.

[2] Alguacil, M., Herranz-Zarzoso, N., Pernías, J.C. *et al.* Academic dishonesty and monitoring in online exams: a randomized field experiment. *J Comput High Educ* 36, 835–851 (2024). https://doi.org/10.1007/s12528-023-09378-x

[3] Alharthi, M., & Alhussain, T. (2024). Cybersecurity governance strategies in higher education: Balancing innovation and risk. Journal of Information Security and Applications, 77, 104612. https://doi.org/10.1016/j.jisa.2024.104612

[4] Alhussain, T., Alruwaili, M., & Alshammari, F. (2023). Leadership commitment and cybersecurity governance in higher education institutions. *Journal of Information Security and Applications, 71*, 103264. https://doi.org/10.1016/j.jisa.2023.103264

[5] Alsadi, A., Kadhim, K., & Abbas, S. (2023). Participatory governance for cybersecurity in universities. *International Journal of Cybersecurity and Education, 5*(2), 45–59. https://doi.org/10.1016/j.ijce.2023.05.003

[6] Alshahrani, F., Alyami, S., & Alqhatani, A. (2025). Exploring cybersecurity challenges of digital transformation in higher education. In *IHSI 2025: Intelligent Human Systems Integration*.

[7] Arumugam, K. J. (2024). Behind the Cloud: Uncovering Critical Security Threats. Available at SSRN 5160686.

[8] Balash, D. G., Kim, D., Shaibekova, D., Fainchtein, R. A., Sherr, M., & Aviv, A. J. (2021). Examining the examiners: Students' privacy and security perceptions of online proctoring services. https://arxiv.org/abs/2106.05917

[9] Chantal, M., Shengnan, H., Olga, V., & Cerratto-Pargman, T. (2023). Privacy as contextual integrity in online proctoring systems in higher education: A scoping review. https://arxiv.org/abs/2310.18792

[10] David, A., et al. (2025). Privacy in online proctoring systems in higher education: Stakeholders' perceptions, awareness, and responsibility. Journal of Computing in Higher Education. https://link.springer.com/article/10.1007/s12528-025-09461-5

[11] Feng, H., & Wang, Y. (2024). Embedding digital ethics and cybersecurity awareness in university curricula. Computers in Human Behavior, 155, 108002. https://doi.org/10.1016/j.chb.2024.108002

[12] Feng, H., Liu, Y., & Zhang, S. (2024). Embedding cybersecurity education into university curricula: A longitudinal study. *Computers in Human Behavior, 147*, 107936. https://doi.org/10.1016/j.chb.2023.107936

[13] Gupta, S. L., Kishor, N., Mishra, N., Mathur, S., & Gupta, U. (2022). *Digitalization of Higher Education using Cloud Computing: Implications, Risk, and Challenges.* Chapman & Hall / Routledge.

[14] Hassan, S., & Verma, R. (2023). Promoting institutional trust through comprehensive cyber resilience. International Journal of Educational Technology, 21(2), 78–95. https://doi.org/10.1007/s40692-023-00215-7

[15] Heinrich, E. (2025). A systematic-narrative review of online proctoring systems and a case for open standards. *Open Praxis*, *17*(3), 485-499.

[16] Hughes, C., & Robinson, N. (2024). Effective vulnerability management: *managing risk in the vulnerable digital ecosystem*. John Wiley & Sons

[17] Ilori, O., Nwosu, N., & Naiho, H. N. (2024). Third-party vendor risks in IT security: A comprehensive audit review and mitigation strategies. World Journal of Advanced Research and Reviews, 22(3), 213–224. https://www.researchgate.net/publication/381844798

[18] Kaur, P., & Farooq, A. (2023). Participatory oversight in digital governance for universities. Education and Information Technologies, 28, 3670–3685. https://doi.org/10.1007/s10639-023-11755-8

[19] Kaur, P., & Singh, R. (2023). Oversight, transparency, and accountability in institutional cybersecurity governance. *International Journal of Information Management, 71*, 102670. https://doi.org/10.1016/j.ijinfomgt.2023.102670

[20] Li, J., et al. (2023). Identification of key factors affecting data breach incidents in higher education. PMC. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10228450/

[21] Li, X., Zhang, J., & Chen, M. (2024). Integrating governance, technical safeguards, and capacity building for HEI resilience. Journal of Cybersecurity Studies, 10(1), 33–50. https://doi.org/10.1080/2573234X.2024.1184970

[22] Mahmoud, H., & Alshammari, F. (2023). Ethical considerations in higher education digital transformation. Computers & Security, 138, 104189. https://doi.org/10.1016/j.cose.2023.104189

[23] Moldstud. (2024). Mitigating cybersecurity risks in university IT operations. https://moldstud.com/articles/p-mitigating-cybersecurity-risks-in-university-it-operations

[24] Moonsamy, A., Ahmed, M., Guidetti, O., & Rashid, B. (2024). The Human Firewall: Mitigating Ransomware Risks in Critical Infrastructures through Human-Centric Approaches. In *Ransomware Evolution* (pp. 192-207). CRC Press.

[25] Mutimukwe, C., Viberg, O., McGrath, C., & Cerratto-Pargman, T. (2025). Privacy in online proctoring systems in higher education: stakeholders' perceptions, awareness and responsibility. Journal of Computing in Higher Education, 1-30.

[26] Nwosu, C., Iahad, N., & Rahim, N. (2023). Addressing human-factor vulnerabilities in university cybersecurity. *Education and Information Technologies, 28*, 3321–3337. https://doi.org/10.1007/s10639-023-11590-2

[27] Pokorny, A., Ballen, C.J., Drake, A.G. "Out of my control": science undergraduates report mental health concerns and inconsistent conditions when using remote proctoring software. Int J Educ Integr 19, 22 (2023). https://doi.org/10.1007/s40979-023-00141-4

[28] Rahman, T., & Ahmed, S. (2024). Building rights-centered digital ecosystems in universities. International Journal of Cyber Education, 7(1), 45–61. https://doi.org/10.1080/2573234X.2024.1184975

[29] Sadiqzade, Z., & Alisoy, H. (2025). Cybersecurity and online education-Risks and solutions. *Luminis Applied Science and Engineering*, 2(1)

[30] Saleh, A., Farouk, M., & Malik, A. (2024). Phased implementation strategies for cyber resilience in resource-constrained universities. Education and Information Technologies, 29, 4090–4108. https://doi.org/10.1007/s10639-024-11845-2

[31] Tsai, H., & Chen, M. (2024). Context-sensitive implementation of digital resilience frameworks in higher education. International Journal of Cyber Education, 6(2), 77–95. https://doi.org/10.1080/2573234X.2024.1184935

[32] Ul Hassan, M., Murtaza, A., & Rashid, K. (2025). Redefining higher education institutions (HEIs) in the era of globalisation and global crises: A proposal for future sustainability. European Journal of Education, 60(1), e12822.

[33] Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet, 13*(2), 39. https://doi.org/10.3390/fi13020039

[34] WatermarkInsights. (2024). 10 best practices for higher education data security. https://www.watermarkinsights.com/resources/blog/10-best-practices-for-higher-education-data-security

[35] Zhang, J., & Li, X. (2024). Protecting digital rights and academic freedom in HEI cyber resilience initiatives. Computers & Education, 206, 104860. https://doi.org/10.1016/j.compedu.2024.104860

[36] Zhang, J., & Wang, X. (2024). Digital ethics and cybersecurity literacy in higher education programs. *Journal of Cyber Education, 9*(1), 12–28. https://doi.org/10.1080/2573234X.2024.1184932.

[37] Zhou, L., & Lee, C. (2024). Technical mitigation strategies for cybersecurity risks in higher education. *Computers & Security, 123*, 102974. https://doi.org/10.1016/j.cose.2024.102974