International Journal for Novel Research in Economics , Finance and Management
www.ijnrefm.com
ISSN:3048-7722
Volume 4, Issue 6, Nov-Dec-2026, PP:01-06

Beyond Technology: Cybersecurity Governance And Human Capacity In AI-Enabled Education — Evidence From A Burundian Secondary School

Dr. Prudence Ndungutse-Mubiria*, Dr. Fouad Yehyab
BSc (Medical Bioscience), PGCE, MA (Educational Leadership),
MBA (International Relations and Diplomacy), PhD (AI and Cybersecurity in Education)

Abstract- As schools in low-resource settings adopt Artificial Intelligence (AI) for personalized learning, they simultaneously take on cybersecurity risks that are rarely examined in the AI-in-education literature. This study investigated the cybersecurity challenges associated with AI adoption at Discovery School, a secondary school in Bujumbura, Burundi. A convergent mixed-methods design combined a structured survey (n = 110: administrators, teachers, students, parents) with semi-structured interviews (n = 35), analyzed in SPSS 27 (descriptive statistics, chi-square test) and NVivo 14 (six-phase thematic analysis, Cohen's κ = 0.83), triangulated through a joint-display approach and interpreted through the NIST Cybersecurity Framework. Cybersecurity readiness was rated only moderately overall (M = 3.19, SD = 0.84) against a backdrop of high perceived AI effectiveness for learning (M = 3.98). Counter-intuitively, administrators (the group with the fullest institutional view) reported the lowest confidence of any stakeholder group (M = 2.80), which is interpreted as informed awareness of governance gaps rather than technical incompetence. A chi-square test confirmed a statistically significant association between having received cybersecurity training and confidence in managing AI-related security risks, $\chi^2(1) = 8.09$, $p = .004$. Qualitative analysis identified Cybersecurity Awareness and Practices as a major theme (16.3% of coded references, 27 interviewees), revealing unclear data-ownership provisions in third-party vendor contracts, the absence of a formal incident-reporting procedure, and a near-total absence of student voice in cybersecurity discussions. Triangulation indicated that the school's central cybersecurity vulnerability is institutional and human rather than purely technological: awareness exists, but detection, response, and recovery capacity does not. The study proposes a governance readiness phase which comprising policy coherence, role clarity, and minimal institutional capacity that should precede the NIST Framework's five core functions in resource-constrained education systems, and offers a prioritized, evidence-based roadmap for schools and policymakers in Burundi and comparable contexts.

Keywords: Cybersecurity; NIST Cybersecurity Framework; Artificial Intelligence in Education; Data Governance; Digital Citizenship; Sub-Saharan Africa; Burundi; Mixed Methods

I. INTRODUCTION

The adoption of artificial intelligence (ai) in schools depends on the collection, storage, and processing of substantial volumes of sensitive student data, exposing educational institutions to cybersecurity risks that conventional digital systems do not carry in the same form: algorithmic manipulation, adversarial attacks, and data breaches affecting learners who are frequently minors (zawacki-richter et al., 2019; Triplett, 2023; berman, geffen, and nelson, 2022). The education sector is generally less prepared for cybersecurity threats than sectors such as finance or health care, in part because schools rarely have the budget or technical expertise available to more heavily regulated industries (williamson and eynon, 2020). These difficulties are compounded in developing countries such as burundi by limited infrastructure, low digital literacy, the absence of a national data-protection statute, and an immature ai-governance policy landscape (halton, 2019; arakaza and mcfarlane, 2023). Discovery school, a private secondary school in bujumbura, has adopted ai-based adaptive learning, automated feedback, and performance-assessment tools, and does so through third-party digital platforms without a documented data-governance policy or a formal incident-reporting procedure. This creates precisely the kind of gap this study set out to examine: what are the main cybersecurity challenges associated with adopting ai technologies in a burundian secondary school, and what does this reveal about the applicability of established cybersecurity governance frameworks in a resource-constrained institutional context? Answering this question matters because institutional integrity, student safety, and stakeholder trust are all put at risk by data breaches, phishing, malware, and privacy violations (tsado, 2019; aldaajeh et al., 2022), And because no prior study had examined cybersecurity governance as a central, rather than peripheral, concern in african ai-in-education research.

International Journal for Novel Research in Economics , Finance and Management
www.ijnrefm.com
ISSN:3048-7722
Volume 4, Issue 6, Nov-Dec-2026, PP:01-06

II. THEORETICAL FRAMEWORK AND RELATED LITERATURE

The nist cybersecurity framework structures the analysis, offering a five-function model (identify, protect, detect, respond, and recover) for managing digital risk (nist, 2018). The framework was designed principally for enterprises in high-income countries already engaged in digital governance; this study examines whether its assumptions hold in an institution with limited technical capacity, informal governance, and no legal data-protection mandate. The wider literature documents ai-specific risks largely absent from earlier cybersecurity scholarship: algorithmic bias, in which ai trained on unrepresentative data returns unfair outcomes; adversarial attacks, in which manipulated inputs are used to deceive ai systems; and algorithmic exploitation, in which platforms are gamed for unfair advantage (berman, geffen, and nelson, 2022; o'neil, 2016; ziosi and pruss, 2024). Phishing and social engineering are reported as particularly effective in low-digital-literacy contexts (triplett, 2023), and regional evidence from kenya, rwanda, and south africa shows that schools with a developed incident-response strategy recover more quickly from cyber incidents (situma, 2025; magunje, 2024; kabanda, 2024). At the policy level, the african union convention on cyber security and personal data protection (2014) provides a regional framework, but enforcement and local adaptation remain limited (african union, 2014). Without a domestic burundian data-protection statute, schools such as discovery school must rely on voluntary adoption of principles such as those found in the gdpr (data minimization, purpose limitation, and defined retention) in the absence of a binding legal requirement to do so (voigt and von dem bussche, 2017). This study contributes empirical evidence on how such a governance vacuum manifests inside one school's daily operations, and on what institutional preconditions are needed before a technically sound framework such as nist's can be meaningfully applied.

III. MATERIALS AND METHODS

TThis study forms part of a broader convergent mixed-methods case study of AI adoption at Discovery School (embedded case study design; Yin, 2018), reported here for the cybersecurity dimension specifically. Quantitative data were collected through a structured survey administered to 110 purposively sampled respondents, stratified by stakeholder role (5 administrators, 20 teachers, 70 students, 15 parents), including a Cybersecurity Awareness and Trust subscale assessing perceptions of digital risk, data protection, access control, and institutional response, adapted from NIST-aligned items (Cronbach's $\alpha = 0.82$). Qualitative data comprised 35 semi-structured interviews analyzed using Braun and Clarke's**With 20%** of transcripts independently double- coded (Cohen's $\kappa = 0.83$). For the cybersecurity dimension specifically, quantitative analysis comprised descriptive statistics for the Cybersecurity Readiness construct and a chi-square test of association between having received cybersecurity training (yes/no) and confidence in responding to AI-related threats (high/low). Qualitative analysis focused on the theme Cybersecurity Awareness and Practices. Ethical clearance and Discovery School's written permission were obtained prior to data collection; all data were pseudonymized, encrypted, and managed according to GDPR-consistent principles.

IV .RESULTS

1.Cybersecurity Readiness by Stakeholder Group

Table 1 shows cybersecurity readiness by stakeholder groups. Cybersecurity readiness was rated only **M**oderately overall ($M = 3.19$, $SD = 0.84$), notably lower than perceived AI effectiveness for learning ($M = 3.98$). Administrators reported the lowest confidence of any stakeholder group ($M = 2.80$, $SD = 0.75$; only 20% agreement that current systems were adequate), despite or rather, in light of the qualitative findings, because of their fuller institutional visibility into governance gaps. Teachers reported moderate concern ($M = 3.16$; personal concern $M = 3.80$) but low confidence in institutional measures ($M = 3.10$) and in their own capability to respond to threats ($M = 3.00$). Students reported moderate trust in data privacy ($M = 3.20$, $SD = 0.96$; 46% agreement), a pattern attributed more to a lack of transparency about data use than to any negative experience. Parents expressed the most pronounced concern of any group ($M = 3.58$; 80% concerned), reflecting heightened sensitivity to their children's data.

International Journal for Novel Research in Economics , Finance and Management
www.ijnrefm.com
ISSN:3048-7722
Volume 4, Issue 6, Nov-Dec-2026, PP:01-06

Table 1. Cybersecurity readiness/confidence by stakeholder group.

Stakeholder group	Cybersecurity Readiness M (SD)	Note
Administrators (n=5)	2.80 (0.75)	Lowest confidence; fullest institutional view
Teachers (n=20)	3.16	Aware of risk, low confidence in response capacity
Students (n=67)	3.20 (0.96)	Moderate trust; transparency gap, not misuse
Parents (n=15)	3.58	Highest concern; data-privacy focused
Overall	3.19 (0.84)	Moderate; trails AI-effectiveness scores (M=3.98)

Ai-effectiveness Scores (M=3.98)

2. Training And Confidence: Chi-square Test

A chi-square test of independence examined the relationship between having received cybersecurity training (yes/no) and confidence in responding to

Ai-related threats (high/low). The association was statistically significant, $\chi^2(1) = 8.09$, P = .004: 80% Of trained staff reported high confidence in responding to ai-related threats, compared with 54.5% Of untrained staff. This finding indicates that the primary lever available for improving cybersecurity confidence at discovery school is human capacity-building rather than additional technology procurement, while the cross-sectional, self-report design means the direction of this association cannot be established with certainty. These results are summarized in table 2 below:

Table 2. Cybersecurity Training × Confidence In responding To Ai-related Threats. $X^2(1) = 8.09$, P = .004.

	High confidence	Low confidence	Row total
Received training (☷ s)	44	11	55
No training (No)	30	25	55
Column total	74	36	110

3.Qualitative Evidence: Cybersecurity Awareness and Practices

Thematic analysis identified Cybersecurity Awareness and Practices as a major theme (16.3% of 171 coded references, 27 interviewees), pointing to policy gaps, insufficient training, privacy concerns, and unclear reporting processes. Administrators identified a specific governance gap: "We use third-party platforms, but the contracts are not clear regarding data ownership. We need clear policies here" (Administrator A4). A teacher described the absence of a formal escalation procedure despite individually responsible behavior: "I got one phishing e-mail last term and I reported it, but there is no formal procedure to log and escalate" (Teacher T7), indicating that cybersecurity practice at Discovery School is currently individualized rather than institutionalized. Parental concern centered on access and trust rather than technical risk as such:"Who can see my child's information? That worries me more than the technology itself" (Parent P3). A striking silence emerged across all 35 interviews: no participant from the student stakeholder group which is the largest group and the primary users of the AI platforms, raised any question about data privacy, cybersecurity, or who could access their personal information, and no participant from any group raised the cost of cybersecurity tools, insurance, or compliance systems.

4. Triangulation

Triangulation of the quantitative and qualitative strands showed complementarity rather than either interviews explained the institutional conditions underlying this relationship, unclear contractual data-ownership provisions,

International Journal for Novel Research in Economics , Finance and Management
www.ijnrefm.com
ISSN:3048-7722
Volume 4, Issue 6, Nov-Dec-2026, PP:01-06

absent incident-reporting procedures, and a governance structure in which teachers regard cybersecurity as an administrative responsibility while administrators regard it as an individual one. Mapped against the NIST Framework, Discovery School shows intermediate maturity in Identify and Protect, but Detect, Respond, and Recover functions remain largely absent, a profile in which digital adoption has outpaced digital governance (Berman, Geffen, and Nelson, 2022).

5. Discussion

1. The counter-intuitive finding that administrators report the lowest cybersecurity confidence is best explained not as incompetence but as institutional visibility: administrators see the whole governance picture such as unclear vendor contracts, absent reporting procedures, that teachers and students, working with a narrower slice of the system, do not. The significant association between training and confidence ($\chi^2(1) = 8.09$, $P = .004$) Confirms that human capacity is a genuine, actionable lever, but the study cannot determine whether training causes confidence or whether already-confident Individuals are more likely to seek training; nor can it determine whether reported confidence reflects genuine technical competence or merely perceived preparedness, since cybersecurity readiness was assessed through self-report rather than technical audit.

These findings extend the nist cybersecurity framework for resource-constrained institutional contexts. The framework's five functions presuppose a baseline of institutional governance capacity that does not yet exist at discovery school: without a documented policy on who owns platform-generated student data, the identify function cannot be meaningfully executed, since the school cannot accurately inventory its digital assets or the responsibilities attached to them. This study therefore proposes a governance readiness phase, comprising three preconditions. First, policy coherence: a clear, documented, and communicated data-governance policy specifying data ownership, third-party sharing conditions, and recourse in the event of a breach. Second, role clarity: an explicit, accepted allocation of cybersecurity responsibility across administrators, it staff, teachers, and students, replacing the current diffusion of responsibility identified in the interviews. Third, minimal institutional capacity: at least one designated data-protection lead with the time and authority to manage cybersecurity, rather than treating it as an unfunded addition to already overstretched administrative roles. Without these three preconditions in place, technical cybersecurity investment is likely to have limited and uneven effect, regardless of the sophistication of the tools procured.

6.. Practical And Policy Implications

For school leaders, the most urgent and lowest-cost action is establishing the governance readiness preconditions described above: naming a data-protection lead, inventorying platforms and the student data they hold, requesting written clarification of data ownership from vendors, and Drafting a one-page incident-reporting procedure specifying whom to notify and how. Because perceived readiness rises significantly with training ($p = .004$), Regular, practical cybersecurity training for staff, not a one-time session, should accompany these governance steps. For policymakers, the absence of a national data-protection law and ai-in-education policy is an active risk rather than a neutral gap: national policy should establish legally binding obligations regarding data rights, consent, and breach notification consistent with the african union convention (2014), alongside minimum institutional governance requirements for any school adopting ai. Given the near-total absence of student voice on this topic, digital-citizenship education that is the informed, critical, and ethical use of digital systems should be built into the curriculum so that students, the largest stakeholder group and primary users of these platforms, are equipped to participate in decisions about their own data.

7. Limitations And Future Research

Cybersecurity readiness in this study was assessed entirely through stakeholder self-report; no technical security audit, network analysis, or review of vendor contracts was conducted, meaning that reported confidence cannot be equated with verified technical security. The cross-sectional design cannot establish whether training causes confidence or whether the reverse, or some third factor, better explains the association. The findings are drawn from a single, urban, comparatively well-resourced private school and may not generalize to rural or public institutions with different governance capacity. An independent technical cybersecurity audit is recommended as the priority next step to validate self-reported confidence against actual security posture, alongside dedicated research into data sovereignty and governance for ai-generated student data in african school systems, and a targeted study designed specifically to elicit Student perspectives on cybersecurity, given their almost complete absence from the present dataset.

International Journal for Novel Research in Economics , Finance and Management
www.ijnrefm.com
ISSN:3048-7722
Volume 4, Issue 6, Nov-Dec-2026, PP:01-06

V. CONCLUSION

Cybersecurity readiness at discovery school trails the enthusiasm generated by ai's pedagogical benefits, and the evidence indicates that the resulting risk is primarily institutional and human rather than technological: awareness of risk exists, but the policy, procedural, and role clarity needed to detect, respond to, and recover from incidents does not. Training meaningfully predicts confidence, but confidence built on training alone is insufficient without the governance readiness such as policy coherence, role clarity, and minimal institutional capacity, proposed here as a precondition for the nist cybersecurity framework's five core functions in resource-constrained education systems. As ai adoption continues to outpace governance in burundian schools, closing this gap is a matter of urgency, not routine institutional housekeeping.

Declarations

- **Funding.** This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.
- **Conflict Of Interest.** The authors declare no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.
- **Ethical approval.** The study received institutional ethical clearance prior to data collection, together with formal written permission from discovery school's leadership. Informed consent was obtained from all adult participants; parental/guardian consent and student assent were obtained for minor participants.
- **Data availability statement.** The datasets generated and analyzed during this study are available from the corresponding author on reasonable request, subject to the confidentiality undertakings given to participants and discovery school.
- **Credit authorship contribution statement.** Prudence ndungutse-mubiri: conceptualization, methodology, investigation, formal analysis, writing – original draft, writing – review & editing. Fouad yehya: supervision, methodology, writing – review & editing.
- **Acknowledgements.** The authors thank the administrators, teachers, students, and parents of discovery school, for their participation and openness.

REFERENCES

1. AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., and Choo, K.-K. R. (2022). The Role of National Cybersecurity Strategies in the Improvement of Cybersecurity Education. Computers & Security, 119, 102754.https://doi.org/10.1016/j.cose.2022.102754
2. Arakaza, A. and McFarlane, D. J. (2023). Digital Connectivity in Burundi and Tanzania: Pathways to Digital Development in Africa (Doctoral dissertation, Thammasat University).
3. Braun, V. and Clarke, V. (2008). Using Thematic Analysis in Psychology. Qualitative Research in Psychology, 3(2), pp. 77–101. https://doi.org/10.1191/1478088706qp063oa
4. Kabanda, M. (2024). Information Security Awareness in sub-Saharan African Schools: The Role of Educational Leadership in Turbulent Times.
5. Kabanda, MN (2024). Information Security Awareness in Sub-Saharan African Schools: The Role of Educational Leadership in Turbulent Times. In T. Choudhry (Ed.), Business, Management and Economics: Vol. 0. Leadership Studies in the Turbulent Business Eco-System [Working Title](Vol. 0). IntechOpen.
6. Magunje, C. and Chigona, W. (2024). Educators' Cybersecurity Vulnerabilities in Marginalized Schools in South Africa. In Annual Conference of South African Institute of Computer Scientists and Information Technologists (pp. 347-360). Cham: Springer Nature Switzerland.
7. NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. [online] Gaithersburg: National Institute of Standards and Technology. Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [Accessed 28 April 2025].
8. Situma, J. (2025). A Framework for Effective ICT Utilization in Teaching in Uganda's secondary schools (Doctoral dissertation, Uganda Martyrs University).
9. Triplett, W. J. (2023). Addressing Cybersecurity Challenges in Education. International Journal of STEM Education for Sustainability, 3(1), pp.47-67.
10. Tsado, L. (2019). Cybersecurity Education: The Need for a Top-Driven, Multidisciplinary Approach. Journal of Cybersecurity Education, Research and Practice, 2019(1), Article

4.https://digitalcommons.kennesaw.edu/jcerp/vol2019/iss1/4

11. Williamson, B. and Eynon, R. (2020). Historical Threads, Missing Links, and Future Directions in AI in Education. Learning, Media and Technology, 45(3), pp. 223–235. https://doi.org/10.1080/17439884.2020.17989 95.
12. Yin, R. K. (2018). Case Study Research and Applications: Design and Methods. 6th ed. Thousand Oaks, CA: SAGE Publications.
13. Zawacki-Richter, O., Marín, V. I., Bond, M., and Gouverneur, F. (2019). Systematic Review of Research on Artificial Intelligence Applications in Higher Education–Where Are the Educators?. International Journal of Educational Technology in Higher Education, 16(1), p.39.