ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 14, Issue 1, pp: (104-109), Month: January - March 2026, Available at: www.researchpublish.com

Evaluating Cybersecurity, Data Protection, and Safe AI Training in a Private Telecommunications Entity in Zimbabwe

[1]Enock Panganayi Mawuye

[1]University of Rwanda,

[2]Henry Mukono, [2]University of Zimbabwe

DOI: https://doi.org/10.5281/zenodo.18536136

Published Date: 09-February-2026

Abstract: **The rapid digital transformation of the telecommunications sector has intensified cybersecurity threats, data protection risks, and ethical challenges associated with artificial intelligence (AI). This study evaluates cybersecurity practices, data protection mechanisms, and safe AI training within a private telecommunications entity in Zimbabwe. Using a mixed-methods research approach, the study assesses organizational preparedness, employee awareness, governance frameworks, and compliance with data protection and emerging AI safety standards. Findings indicate that while foundational cybersecurity controls exist, gaps remain in advanced threat detection, employee training consistency, and structured AI governance. Data protection compliance shows moderate alignment with statutory requirements, though enforcement and staff awareness are uneven. The study concludes that effective cybersecurity and safe AI adoption require integrated governance frameworks, continuous training, and leadership commitment. The article contributes to limited empirical literature on cybersecurity and AI governance in Zimbabwe's private sector and provides practical recommendations for strengthening digital resilience in telecommunications firms.**

Keywords: **Artificial Intelligence, Board Induction, Data Protection, Private Communications Entity, Zimbabwe.**

1. INTRODUCTION

The telecommunications sector plays a pivotal role in modern economies by enabling digital communication, financial transactions, and data-driven services. In Zimbabwe, private telecommunications entities are central to national connectivity, mobile financial services, and digital inclusion. However, the increasing reliance on digital infrastructures has heightened exposure to cybersecurity threats, data breaches, and ethical risks associated with artificial intelligence (AI). As cyberattacks become more sophisticated and data volumes grow exponentially, the need for robust cybersecurity, effective data protection, and safe AI training has become critical.

Cybersecurity refers to the protection of information systems, networks, and data from unauthorized access, attacks, or damage. Telecommunications entities are particularly vulnerable due to their extensive customer databases, real-time data transmission, and reliance on complex network infrastructures. Data protection, on the other hand, focuses on safeguarding personal and sensitive information in line with legal and ethical requirements. In Zimbabwe, the enactment of the Cyber and Data Protection Act has heightened regulatory expectations for private entities handling personal data.

The emergence of artificial intelligence within telecommunications—through applications such as network optimization, fraud detection, customer service chatbots, and predictive analytics—introduces new opportunities and risks. While AI can enhance efficiency and service quality, it also raises concerns regarding algorithmic bias, data misuse, lack of transparency, and accountability. Safe AI training, therefore, refers to the process of equipping employees with knowledge and skills to develop, deploy, and use AI systems responsibly, securely, and ethically.

Despite the growing importance of cybersecurity, data protection, and AI governance, empirical research on these issues within Zimbabwe’s private telecommunications sector remains limited. Most existing studies focus on public sector institutions or financial services, leaving a gap in understanding sector-specific challenges and practices. Furthermore, organizational readiness for AI safety and ethical use remains underexplored in developing economies.

This study seeks to evaluate cybersecurity controls, data protection practices, and safe AI training within a private telecommunications entity in Zimbabwe. Specifically, it examines governance structures, employee awareness, training effectiveness, and compliance with regulatory and ethical standards. By doing so, the study aims to generate evidence-based insights that can inform policy, management practice, and future research.

The article contributes to the literature by integrating cybersecurity, data protection, and AI safety within a single analytical framework, reflecting the interconnected nature of digital risks. It also provides practical implications for private telecommunications firms seeking to enhance digital resilience, regulatory compliance, and responsible AI adoption in an increasingly complex technological environment.

2. LITERATURE REVIEW

Cybersecurity in the Telecommunications Sector

Cybersecurity has emerged as a strategic priority for telecommunications firms due to the sector’s role as a backbone of digital infrastructure. Scholars argue that telecom operators are prime targets for cyberattacks because they manage large volumes of sensitive data and critical national infrastructure (Von Solms & Van Niekerk, 2013). Common threats include network intrusions, ransomware attacks, insider threats, and distributed denial-of-service (DDoS) attacks.

Effective cybersecurity frameworks emphasize a combination of technical controls, organizational policies, and human factors. Technical measures include firewalls, intrusion detection systems, encryption, and access controls, while organizational measures involve governance structures, incident response plans, and risk management processes. However, studies consistently highlight that human error remains a leading cause of cybersecurity incidents, underscoring the importance of employee training and awareness.

Data Protection and Regulatory Compliance

Data protection is closely linked to cybersecurity but focuses specifically on the lawful and ethical handling of personal data. Globally, data protection regulations such as the General Data Protection Regulation (GDPR) have influenced national legal frameworks. In Zimbabwe, the Cyber and Data Protection Act provides the legal basis for regulating data collection, processing, storage, and sharing.

Literature suggests that compliance with data protection laws requires more than formal policies; it demands organizational culture change, continuous training, and leadership commitment (Cavoukian, 2011). Telecommunications firms face particular challenges due to high data volumes, third-party data sharing, and cross-border data flows. Weak enforcement, limited technical expertise, and low employee awareness often undermine effective compliance in developing economies.

Artificial Intelligence in Telecommunications

AI adoption in telecommunications has accelerated in areas such as network traffic optimization, predictive maintenance, customer analytics, and fraud detection. AI systems rely heavily on large datasets, making data governance and cybersecurity integral to their safe use. Scholars argue that AI amplifies existing cybersecurity and data protection risks by increasing system complexity and reducing transparency (Floridi et al., 2018).

Safe and Ethical AI Training

Safe AI training refers to structured educational initiatives that promote ethical, transparent, and secure AI use. This includes understanding algorithmic bias, data privacy, explainability, accountability, and cybersecurity risks associated with AI systems. The literature highlights that organizations often adopt AI technologies faster than they develop governance and training frameworks, creating ethical and security gaps.

Responsible AI frameworks emphasize principles such as fairness, accountability, transparency,and human oversight. However, translating these principles into practice remains challenging, particularly in contexts with limited regulatory guidance and technical capacity.

Integrating Cybersecurity, Data Protection, and AI Governance

Recent studies advocate for an integrated approach to digital governance, recognizing that cybersecurity, data protection, and AI safety are interdependent. Weak cybersecurity undermines data protection, while poor data governance compromises AI system integrity. Integrated governance models promote coordinated policies, cross-functional collaboration, and continuous capacity building.

In developing countries, resource constraints, skills shortages, and evolving regulatory environments complicate implementation. Nonetheless, scholars emphasize that proactive governance and training investments yield long-term benefits by reducing risk exposure and enhancing organizational trust.

3. RESEARCH METHODOLOGY

Research Design

This study adopts a mixed-methods research design, combining quantitative and qualitative approaches to comprehensively evaluate cybersecurity, data protection, and safe AI training within a private telecommunications entity in Zimbabwe. The mixed-methods approach allows for triangulation of findings, enhancing the depth and credibility of results.

Research Population and Sampling

The study population comprised employees from key functional areas, including information technology, cybersecurity, data analytics, legal/compliance, and operations. A purposive sampling technique was used to select participants with direct involvement in cybersecurity management, data handling, and AI-related processes. This ensured that respondents possessed relevant knowledge and experience.

Data Collection Methods

Primary data were collected using two instruments:

1. Structured Questionnaires

Questionnaires were administered to employees to assess awareness levels, training exposure, perceived effectiveness of cybersecurity controls, data protection practices, and AI safety measures. Likert-scale questions enabled quantitative analysis of perceptions and practices.

2. Semi-Structured Interviews

In-depth interviews were conducted with selected managers and specialists to gain qualitative insights into governance structures, challenges, and strategic priorities related to cybersecurity and AI.

Secondary data were obtained from internal policy documents, training manuals, and publicly available regulatory guidelines.

Data Analysis

Quantitative data were analysed using descriptive statistics to identify trends in awareness, training effectiveness, and compliance levels. Qualitative data were analysed thematically, focusing on governance, risk management, training adequacy, and ethical considerations.

Validity, Reliability, and Ethical Considerations

Instrument validity was enhanced through expert review, while reliability was ensured using consistency checks. Ethical considerations included informed consent, confidentiality, and anonymity of respondents.

Limitations

This study is subject to several limitations that should be considered when interpreting the findings. First, the research focuses on a single private telecommunications entity, which limits the generalizability of results across the entire telecommunications sector in Zimbabwe or other developing economies. Organizational practices and maturity levels may vary significantly among firms.

Second, reliance on self-reported data introduces the possibility of response bias, as participants may overstate compliance levels or training effectiveness. Although triangulation with interviews and document analysis mitigated this risk, some subjectivity remains.

Third, the rapidly evolving nature of cybersecurity threats and AI technologies means that findings represent a snapshot in time. Changes in regulatory frameworks, technologies, or organizational strategies may affect the relevance of results over time.

Despite these limitations, the study provides valuable exploratory insights into cybersecurity, data protection, and safe AI training within a critical sector and lays a foundation for future large-scale and longitudinal studies.

Findings

Cybersecurity Governance and Controls

Findings reveal that the telecommunications entity has established foundational cybersecurity controls, including network firewalls, access management systems, and incident response protocols. However, advanced threat detection and continuous monitoring capabilities were reported as limited. While senior management recognizes cybersecurity as a strategic risk, operational implementation varies across departments.

Employees demonstrated moderate awareness of cybersecurity policies, but training frequency and depth were inconsistent. Technical staff exhibited higher awareness compared to non-technical employees, indicating uneven risk exposure.

Data Protection Practices

The organization has formal data protection policies aligned with Zimbabwe's Cyber and Data Protection Act. Data classification and access controls are in place, but enforcement remains uneven. Several respondents indicated uncertainty regarding data retention policies and third-party data sharing arrangements.Training on data protection is largely compliance-driven and infrequent, reducing its effectiveness in shaping day-to-day behaviour. As a result, data protection practices are often reactive rather than proactive.

Safe AI Training and Governance

AI applications are increasingly used for customer analytics and network optimization. However, the study found no comprehensive AI governance framework. Safe AI training is limited and informal, focusing primarily on technical functionality rather than ethical, legal, and security implications.

Employees involved in AI development expressed concerns about data bias, explainability, and accountability. Non-technical staff reported minimal understanding of AI-related risks, highlighting a significant knowledge gap.

Integration of Cybersecurity, Data Protection, and AI

The study found limited integration between cybersecurity, data protection, and AI governance functions. Responsibilities are siloed, reducing coordination and holistic risk management. This fragmentation weakens organizational resilience and increases exposure to compound digital risks.

4. DISCUSSION OF FINDINGS

The findings indicate that while the telecommunications entity has taken important steps toward strengthening cybersecurity and data protection, significant gaps remain in integration, training depth, and AI governance. The presence of basic controls reflects regulatory compliance, but uneven implementation limits effectiveness.

The limited scope of safe AI training aligns with global concerns that organizations adopt AI faster than governance frameworks evolve. The lack of structured AI ethics and security training increases the risk of unintended consequences, including biased decision-making and data misuse.

The siloed nature of governance structures undermines holistic risk management. Integrating cybersecurity, data protection, and AI governance is essential for managing interdependent risks. The findings underscore the need for strategic alignment, continuous training, and leadership-driven governance reforms.

5. RECOMMENDATIONS

The study recommends the development of an integrated digital governance framework that aligns cybersecurity, data protection, and AI governance. The organization should institutionalize continuous training programs covering cybersecurity awareness, data protection compliance, and safe AI principles for all employees.

Establishing a formal AI governance committee responsible for ethical oversight, risk assessment, and policy development is essential. Advanced cybersecurity tools such as real-time monitoring and AI-driven threat detection should be adopted to enhance resilience.

Leadership commitment is critical; senior management should champion digital risk governance and allocate adequate resources. Regular audits and assessments will ensure continuous improvement and compliance.

6. CONCLUSION

This study evaluated cybersecurity, data protection, and safe AI training within a private telecommunications entity in Zimbabwe, revealing moderate maturity levels alongside critical gaps. While foundational controls and policies exist, inconsistent training, limited AI governance, and fragmented oversight weaken digital resilience. The findings highlight the interconnected nature of cybersecurity, data protection, and AI safety and the need for integrated governance approaches. Strengthening training, enhancing coordination, and institutionalizing responsible AI practices are essential for mitigating emerging digital risks. The study contributes to limited empirical literature on digital governance in Zimbabwe’s private sector and provides actionable insights for strengthening secure, ethical, and resilient telecommunications operations in an increasingly AI-driven environment.

REFERENCES

[1] Cavoukian, A. (2011). Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario.

[2] Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. Minds and Machines, 28(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5

[3] International Telecommunication Union. (2020). Global cybersecurity index 2020: Measuring commitment to cybersecurity. ITU.

[4] ISO/IEC. (2018). ISO/IEC 27001: Information security management systems—Requirements. International Organization for Standardization.

[5] ISO/IEC. (2023). ISO/IEC 23894: Artificial intelligence—Risk management. International Organization for Standardization.

[6] Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. Journal of Financial Economics, 3(4), 305–360. https://doi.org/10.1016/0304-405X(76)90026-X

[7] Kshetri, N. (2018). 1 Blockchain’s roles in strengthening cybersecurity and protecting privacy. Telecommunications Policy, 42(10), 805–817. https://doi.org/10.1016/j.telpol.2018.09.003

[8] Mhlanga, D., & Moloi, T. (2020). COVID-19 and the digital transformation of public sector service delivery in Zimbabwe. African Journal of Governance and Development, 9(1), 1–16.

[9] National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). U.S. Department of Commerce.

[10] Organisation for Economic Co-operation and Development. (2019). Artificial intelligence and data protection: Delivering sustainable AI. OECD Publishing.

[11] Organisation for Economic Co-operation and Development. (2021). Digital security risk management. OECD Publishing.

[12] Republic of Zimbabwe. (2021). Cyber and Data Protection Act [Chapter 12:07]. Government Printer.

[13] Sarker, I. H. (2021). Cybersecurity: Threats, attacks, and mitigation approaches. Journal of Advanced Research, 28, 1–15. https://doi.org/10.1016/j.jare.2020.07.005

[14] Shackelford, S. J., Raymond, A., & Charoen, D. (2020). Cybersecurity risk management: Toward a global harmonization. Minnesota Journal of International Law, 29(1), 1–50.

[15] Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

[16] World Bank. (2020). Data protection and cybersecurity laws in Africa: A comprehensive review. World Bank Group.

[17] World Economic Forum. (2020). Resetting digital trust: Decision-maker’s guide to cybersecurity. WEF.

[18] World Economic Forum. (2021). Global AI governance: Aligning AI systems with human values. WEF.