



**The Copperbelt University, Directorate of Distance Education and Open Learning P.O. Box 21692, Jambo Drive, Riverside, Kitwe, Zambia.**

**Milton Kaoma, Tapati C. Sarmah**

### **ABSTRACT**

This study analysed the effects of cybersecurity risks on telecommunication vendors and mobile network providers (MNOs) during project implementation in Zambia and suggested ways to improve security procedures. The study was conducted in Lusaka involving two major telecommunication vendors particularly Huawei Technologies and ZTE as well as MNOs including Airtel, Zamtel, MTN and Zed Mobile. The sample size which was obtained using purposive sampling comprised a total of 63 respondents consisting of 22 IT and cybersecurity personnel, 05 project managers, 10 Huawei and ZTE procurement and vendor management staff, 16 telecommunications engineers and field technicians and 10 procurement and contract officers. Using semi-structured interviews, several risks are mostly caused by human shortcomings, insufficient access restrictions, and deficiencies in vendor supervision and governance. Global frameworks like NIST and ISO 27001 provide guidelines, but local resource and capacity constraints frequently limit their immediate applicability. Therefore, the research emphasises the necessity of context-specific strategies that incorporate continuing monitoring across all project phases, strong technical protections, ongoing awareness training, and stronger governance structures. Overall, the study concludes that enhancing cybersecurity in Zambia's telecommunications sector requires a holistic, adaptive, and collaborative strategy aligned with local organisational realities.

**Keywords:** Cybersecurity, Project Implementation, Telecommunications Vendors, Mobile Network Operators, Cyber Threats

## 1. Introduction

The telecommunications sector has undergone rapid digital transformation over the past decade, driven by the expansion of broadband networks, mobile technologies, cloud computing, and data-driven services. While these developments have improved connectivity and service delivery, they have simultaneously increased exposure to cybersecurity threats. Alshaikh (2020) notes that modern digital infrastructures are characterized by interdependence and complexity, making them particularly vulnerable to cyberattacks that exploit both technical weaknesses and organizational gaps.

Project implementation represents one of the most vulnerable phases within the telecommunications lifecycle. During this stage, systems are actively configured, integrated, and tested, often involving temporary access privileges, legacy system interfaces, and close collaboration between vendors and MNOs. Kerzner (2019) argues that project environments frequently prioritise speed, cost, and scope, inadvertently relegating cybersecurity considerations to a secondary concern. As a result, vulnerabilities introduced during implementation may persist into operational phases, creating long-term security risks.

Telecommunications vendors play a central role in this context. According to Cremer, Hofmann, and Akande (2022), vendors are often granted privileged access to critical systems and data, effectively extending the cybersecurity perimeter of MNOs beyond organisational boundaries. In Zambia, international vendors such as Huawei and ZTE are deeply embedded in network rollout, maintenance, and upgrade projects. Consequently, cybersecurity failures at the vendor level have direct implications for project outcomes, service continuity, and national digital resilience.

At the policy level, Zambia has taken steps to strengthen its cybersecurity posture through legislative instruments such as the Cyber Security and Cyber Crimes Act of 2021. However, as observed by ZICTA (2023), enforcement capacity, technical expertise, and organisational readiness remain uneven across the sector. This gap between regulatory intent and operational reality underscores the need for empirical research examining how cybersecurity threats manifest during project implementation and how organisations respond to them. This study addressed that gap by focusing on telecommunications vendors and MNOs operating in Zambia.

## 2. Literature Review

### 2.1 Cybersecurity Risks in Telecommunications Projects

Globally, the cybersecurity risks faced in telecom projects have increased significantly in both scale and complexity. According to Wang, Ho, and Shan (2024), firms in digitized sectors are encountering heightened cyber threats that adversely affect innovation and productivity. Their quantitative model highlights severe risks but does not adequately capture real-world project dynamics, such as data breaches within vendor environments and software supply chains. Complementary industry analyses from PwC (2025) and Corporate Compliance Insights (2024) reveal that over 60% of corporate cybersecurity incidents stem from third-party and vendor-related breaches, highlighting the exploitation of trust in supplier relationships for cybersecurity attacks. While these documents provide descriptive evidence, they lack the methodological rigor associated with peer-reviewed research, necessitating careful academic analysis.

Mobile Network Operators (MNOs) often rely on third-party vendors for network equipment and services. Gupta et al. (2024) propose blockchain-enabled vendor assurance mechanisms to enhance supply chain security, providing an innovative tracking system for vendor integrity, though it presumes high digital maturity and interoperability, which may not be achievable in developing countries. Ilter (2024) also emphasizes due diligence, contractual obligations, and certification audits as risk mitigation strategies, noting that while these recommendations are plausible, their effectiveness is constrained by a lack of field validation regarding actual project outcomes.

Cesarano et al. (2025) present a technical framework aimed at addressing edge network vulnerabilities and firmware attacks during project deployment, revealing that cybersecurity failures often stem from weak system architectures rather than negligence. However, their findings are based solely on laboratory simulations, leaving open questions about the applicability of these strategies in resource-constrained telecom environments. Bernardo (2025) attempts to link organisational cybersecurity maturity with governance frameworks, such as the NIST Cybersecurity Framework, but his assessment assumes uniform regulatory enforcement, which is often absent in many African contexts.

In critique, while international studies offer various models and solutions, they frequently ignore the organisational and infrastructural realities affecting telecom projects in developing nations,

suggesting a need for localized assessments, like those centered on Zambia's telecom vendors and MNOs.

## **2.2 Effects of Cybersecurity Threats on Project Implementation**

Telecom operators depend significantly on third-party vendors for essential infrastructure, which introduces vulnerabilities that can cascade into broader network risks. Cybersecurity incidents have been shown to have various adverse effects on telecom projects, including operational disruptions, increased costs, and harm to vendor credibility. Research by Savunen (2024) and Corporate Compliance Insights (2024) indicates that compromised vendor networks contribute to project delays, reduced network performance, and reputational damage for both the primary contractor and the client, typically MNOs. This sentiment is mirrored by Cremer et al. (2022), whose systematic review emphasized that cyber threats not only delay project timelines but also create enduring maintenance difficulties, although they noted the absence of project-specific causal data which makes quantifying the economic impact in developing regions challenging.

In the African context, many local vendors are reportedly unprepared for advanced cyberattacks, as discussed by Ncube and Ngulube (2022), who highlighted their reliance on improvised methods to combat threats affecting MNO operations. An assessment by GFCE/KPMG (2023) noted that weak governance and fragmented regulations exacerbate cyber incidents, though the study does not clearly connect these governance issues to tangible project-level consequences. Abass and Osei-Tutu (2023) further elucidate that inconsistent national frameworks across Sub-Saharan Africa impede uniform compliance among vendors. Their findings, while robust, fail to account for specific national nuances, such as Zambia's unique policy landscape.

Local research within Zambia, including the studies by Mwila (2020) and ZICTA (2023), provides a more nuanced perspective, indicating that cyber threats frequently arise from inadequate vendor training, poor authentication processes, and lack of monitoring capabilities during projects. Mwila's qualitative research illustrates that breaches can lead to network downtimes, subsequently delaying service launches and inflating operational costs. Despite the small sample sizes limiting the generalizability of these findings, the ICT Journal Zambia (2024) notes that descriptive insights abound, particularly emphasizing the challenges vendors face with tools and financing for security measures. Collectively, while global literature establishes the risks associated with

telecommunications networks, African and Zambian studies elaborate on the specific manifestations and implications of those risks.

### **2.3 Cybersecurity Governance and Mitigation Approaches**

Mitigation measures in cybersecurity literature focus on three main pillars: technical controls, contractual mechanisms, and human capacity development. Advocates like Ilter (2024) and Gupta et al. (2024) stress the importance of incorporating cybersecurity clauses into procurement contracts, including mandatory compliance audits and vendor liability clauses. However, these recommendations may be unrealistic given the lower sophistication of vendors in Zambia's telecom sector. Bernardo's (2025) cyber maturity model suggests a phased capacity development approach, yet it may demand too many resources from smaller vendors typical in African telecoms. Recommendations by Cesarano et al. (2025) for technical interventions, such as secure firmware validation and edge encryption, offer solid defense mechanisms but require substantial investment and skilled personnel. In contrast, GFCE/KPMG (2023) promote scalable, cost-effective solutions like shared cybersecurity infrastructure and regional training programmes.

The Zambian ICT Journal (2024) supports the need for simpler cybersecurity frameworks and compliance with data protection laws, emphasizing targeted training to enhance local vendor readiness. Critically, while many global frameworks propose comprehensive controls, they often overlook local budget constraints and enforcement issues. In comparison, African scholars emphasize systemic readiness and gradual improvements, leading to the suggestion that the best mitigation approach is a hybrid model that merges global standards, like NIST frameworks, with tailored solutions such as vendor training and adaptive procurement practices.

### **3. Methodology**

This study adopted a qualitative research design to explore cybersecurity threats within their organisational and project contexts. Creswell (2013) asserts that qualitative approaches are particularly effective for examining complex social and technical phenomena where meaning is constructed through participant experience.

Purposive sampling was used to select 63 participants from Huawei Technologies Zambia, ZTE, and four licensed MNOs including MTN, Airtel, Zamtel, and Zedmobile. Participants included cybersecurity specialists, IT managers, project managers, procurement officers,

telecommunications engineers, and field technicians. This diversity enabled triangulation of perspectives across technical, managerial, and governance roles.

Data were collected through semi-structured interviews, allowing participants to elaborate on their experiences while ensuring alignment with the study objectives. Thematic analysis was conducted following Sarantakos' (1998) analytical framework, enabling the identification of recurring patterns and relationships. Ethical considerations were addressed in accordance with Kombo and Tromp (2006), with informed consent and confidentiality

## **4. Findings**

### **4.1 Prevalence of Cybersecurity Risks Affecting Telecommunications Vendors**

The findings reveal that cybersecurity risks are a persistent challenge during telecommunications project implementation. Respondents across both vendors and MNOs reported frequent exposure to cyber threats arising from increased system interconnectivity, remote access, and reliance on digital project management platforms.

Respondents identified several cybersecurity risks as illustrated in Figure 1. However, three cybersecurity risks were recognized as dominant: data breaches had 35% of the responses, while ransomware attacks had 32% of the responses, and supply chain-related attacks was the third dominant response with 29%. These risks were reported to affect both vendor-managed systems and shared project environments, indicating that cybersecurity threats extend across organisational boundaries.

Furthermore, participants noted that the likelihood of cybersecurity incidents increased during projects involving network upgrades, system integrations, and deployment of new technologies. Such projects typically require elevated access privileges and rapid configuration changes, which respondents perceived as heightening exposure to cyber threats.

Figure 1: Major Security Risks



Source: Survey Data (2025)

### 4.3 Project Phases Most Affected by Cybersecurity Threats

The findings indicate that cybersecurity threats are most prevalent during the project execution phase with 42% of the responses, followed by the initiation and planning phases with 26% and 23% of the responses respectively (Figure 2). The execution phase was identified as the most vulnerable due to activities such as system configuration, data migration, integration testing, and on-site deployment.

Figure 2: Vulnerable Stages to Cybersecurity Risks in Project Implementation

STAGE	FREQUENCY	PERCENTAGE
Initiation	11	26
Planning	10	23
Execution	18	42
Monitoring and Control	03	07
Closure	01	02

Source: Survey Data (2025)

Respondents reported that during execution, cybersecurity controls were sometimes relaxed to meet tight deadlines. Temporary access accounts were created for project personnel and, in some

cases, not promptly revoked after task completion. This practice increased the risk of unauthorised access and system compromise.

The initiation phase was also identified as vulnerable by 11 respondents (26%), particularly where cybersecurity risk assessments were not comprehensively conducted at project inception. Participants noted that cybersecurity was not always explicitly included in project risk registers or scope documents, limiting early identification of potential threats.

#### **4.4 Effects of Cybersecurity Threats on Project Implementation**

Cybersecurity threats were found to have significant negative effects on project implementation. The most commonly reported effects included project delays, operational disruptions, increased costs, and reputational damage.

Project delays occurred when systems had to be taken offline for investigation, malware removal, or security audits. Respondents explained that even minor cybersecurity incidents could result in cascading delays due to task interdependencies within projects. Financial impacts included costs associated with system recovery, additional cybersecurity controls, and compliance requirements.

Reputational damage was particularly pronounced for telecommunications vendors. Participants reported that cybersecurity incidents could weaken trust between vendors and MNOs, affecting ongoing collaborations and future contract awards. In some cases, vendors faced increased scrutiny or termination of project engagements following security incidents.

#### **4.5 Cybersecurity Mitigation Measures Adopted by Vendors and MNOs**

Participants reported a range of mitigation measures currently employed to manage cybersecurity risks during project implementation. As indicated in Table 1, these included access control measures such as encryption of sensitive data, regular system patching, and the use of antivirus and intrusion detection tools were mentioned by 50 respondents signifying 19% of the responses. Sensitisation was also mentioned by 41 respondents denoting 15% whereas technical controls was indicated by 48 responses representing 18%.

Table 1: Mitigation Measures

THEME	FREQUENCY	PERCENTAGE
Sensitisation	41	15
Training	55	20
Continuous Awareness Programmes	42	16
Technical Controls	48	18
Access Control Measures	50	19
Incident Response Planning and Stakeholder Engagement Practices	35	12

Source: Survey Data (2025)

Additionally, cybersecurity awareness training in programmes such as ISO 27001 and NIST was also reported by 42 respondents (16%), although respondents indicated that such training was often conducted periodically rather than continuously. Fifty-five respondents (20%) suggested training in ISO 31000 especially at managerial level. Vendor audits and contractual cybersecurity clauses were equally identified as additional controls; however, their enforcement was described as inconsistent. Lastly, 35 respondents denoting 12% pointed to the presence of incident response planning and stakeholder engagement practices aimed at ensuring coordinated action during security events.

Several participants noted that cybersecurity responsibilities were often separated from project management functions. As a result, cybersecurity considerations were not always fully integrated into project planning, execution, and monitoring processes.

## 5. Discussion

This study set out to examine cybersecurity threats affecting telecommunications vendors and MNOs during project implementation in Zambia and to assess how these threats influence project performance.

### 5.1 Dominance of Technical Cybersecurity Threats in Vendor-Driven Projects

The findings indicate that data breaches and ransomware attacks are the most prevalent cybersecurity threats affecting telecommunications project implementation. This aligns closely with the assertions of Alshaikh (2020), who identifies data breaches as the most persistent

organisational cybersecurity challenge due to weak access controls and insufficient security awareness. Similarly, ENISA (2022) characterises ransomware as one of the fastest-growing threats to telecommunications infrastructure, particularly during periods of system change such as network upgrades and new deployments.

However, this study extends existing literature by demonstrating that these technical threats are not isolated technological failures but are embedded within project implementation dynamics. While PMI (2021) acknowledges that projects introduce temporary vulnerabilities, the present findings show that vendor-led implementations amplify these risks due to the multiplicity of actors accessing systems simultaneously. This supports Kerzner's (2019) argument that project environments inherently fragment accountability, making consistent cybersecurity enforcement difficult.

In the Zambian context, respondents noted that aggressive project timelines often resulted in relaxed access controls and delayed patching. This observation adds empirical weight to Cremer et al.'s (2022) contention that cybersecurity risks are frequently subordinated to delivery pressures in project-based organisations, particularly where contractual penalties prioritise speed over security.

## **5.2 Supply Chain Vulnerabilities and the Expansion of the Cyber-Attack Surface**

One of the most significant findings of this study is the prominence of supply chain-related cybersecurity threats. Participants consistently highlighted vendor access to core systems as a critical vulnerability, reinforcing the growing body of literature on third-party cyber risk. Sharma and Chen (2021) argue that vendors often operate outside the direct governance structures of MNOs, creating blind spots in cybersecurity oversight. Ilter (2024) further demonstrates that attackers increasingly exploit trusted vendor relationships to bypass perimeter defences.

The findings not only corroborate these studies but also provide contextual depth by illustrating how supply chain risks manifest during telecommunications project implementation in a developing-country setting. Unlike many studies that focus on post-deployment operations, this research shows that supply chain vulnerabilities are most acute during project execution phases when temporary access privileges are widely granted. This observation complements PwC's (2025) global findings while highlighting that vendor risk management remains underdeveloped in Zambia due to limited auditing capacity and reliance on vendor self-assessments.

Importantly, this study reveals that supply chain cybersecurity risk is not solely technical but contractual and governance-related. While ISO/IEC 27001 advocates supplier security controls, respondents reported that security clauses in vendor contracts were often generic and weakly enforced. This supports Bernardo's (2025) critique that compliance-oriented approaches fail to address operational realities, particularly in contexts with limited enforcement capacity.

### **5.3 Human Factors and Organisational Behaviour in Cybersecurity Failures**

Beyond technical vulnerabilities, the study highlights the critical role of human factors in cybersecurity incidents. Phishing attacks and credential misuse were frequently cited as entry points for ransomware and data breaches. These findings strongly support Alshaikh's (2020) behavioural cybersecurity framework, which argues that cybersecurity culture is a decisive factor in organisational resilience.

While ENISA (2022) acknowledges human error as a common threat vector, this study provides deeper insight into how human factors interact with project pressures. Respondents described scenarios where project staff prioritised task completion over security protocols, echoing Kerzner's (2019) observation that project environments often encourage risk-taking behaviours under deadline pressure. This reinforces the argument that cybersecurity awareness programmes must be integrated into project management processes rather than treated as standalone initiatives.

In the Zambian telecommunications sector, skills shortages further exacerbate human-related risks. The findings align with GFCE and KPMG (2023), who identify limited cybersecurity skills as a major constraint across African digital ecosystems. However, this study extends the literature by demonstrating that skills gaps are particularly consequential during project implementation, where staff must make rapid security-related decisions in dynamic environments.

### **5.4 Impact of Cybersecurity Threats on Project Performance**

The study confirms that cybersecurity incidents have far-reaching effects on project implementation, including delays, cost overruns, operational disruptions, and reputational damage. Moltke and Xu (2022) argue that cyber incidents disrupt project workflow by diverting resources toward incident response and recovery. The present findings provide empirical confirmation of this dynamic, with respondents reporting halted project activities and extended timelines following security incidents.

Financial and contractual consequences were also prominent. Consistent with Kshetri (2019), respondents noted increased costs associated with audits, system remediation, and regulatory compliance. Moreover, the reputational impact identified in this study aligns with Suzuki's (2020) assertion that trust erosion can outweigh direct financial losses in telecommunications markets. Notably, several participants reported that cybersecurity incidents affected future vendor selection, highlighting long-term strategic consequences that are often underemphasised in project management literature.

### **5.5 Applicability of Global Cybersecurity Frameworks in the Zambian Context**

Although global frameworks such as the NIST Cybersecurity Framework and ISO/IEC 27001 and 31000 were referenced by participants, their implementation was often partial and inconsistent. This finding reflects broader critiques within the literature regarding the contextual relevance of global cybersecurity standards. Bernardo (2025) argues that such frameworks assume stable funding, skilled personnel, and mature governance structures, conditions that are not always present in developing economies.

Abass and Osei-Tutu (2023) similarly advocate for adaptive cybersecurity governance models tailored to local realities. The findings of this study support this perspective, demonstrating that organisations in Zambia selectively adopt elements of global frameworks rather than full-scale implementation. This selective adoption, while pragmatic, creates uneven cybersecurity coverage across project phases.

## **6. Conclusion**

This study demonstrates that cybersecurity threats significantly affect project implementation among telecommunications vendors and MNOs in Zambia. Data breaches, ransomware attacks, and supply chain vulnerabilities disrupt project timelines, increase costs, and undermine organisational trust. Addressing these challenges requires embedding cybersecurity within project governance structures and adapting global frameworks to local institutional capacities. By foregrounding vendor–MNO relationships, this study contributes empirical insights to cybersecurity and project management literature, particularly within developing-country contexts.

## **7 Recommendations**

The study makes the following recommendations:

1. Strengthen human-centric security capacity
2. Implement robust access controls and technical safeguards
3. Embed cybersecurity requirements in governance and vendor management
4. Integrate continuous risk assessment throughout the project lifecycle
5. Enhance incident response and recovery capabilities
6. Invest in advanced security technologies
7. Strengthen collaboration between vendors and telecommunications operators
8. Develop a security-focused organisational culture

## References

- Abass, K., & Osei-Tutu, E. (2023). Cybersecurity governance and resilience in Sub-Saharan Africa. *African Journal of Information Systems*, 15(2), 112–130.
- Alshaikh, M. (2020). Developing cybersecurity culture. *Computers & Security*, 97, 101957.
- Bernardo, R. (2025). Cybersecurity maturity and governance alignment. *Journal of Information Security Management*, 34(1), 45–62.
- Cesarano, C., D'Alessandro, S., & De Nicola, A. (2025). 'Cybersecurity of edge systems: Trends, challenges, and future research.' *Applied Sciences*, 15(1), pp. 335–349.
- Corporate Compliance Insights. (2024). The expanding vendor risk landscape in telecommunications. <https://www.corporatecomplianceinsights.com>
- Cremer, F., Hofmann, R., & Akande, M. (2022). Cyber risk and project management. *International Journal of Project Management*, 40(9), 1121–1135.
- Creswell, J. W. (2013). *Qualitative inquiry and research design* (3rd ed.). Thousand Oaks: Sage.

- ENISA (2022). *ENISA Threat Landscape 2022*. European Union Agency for Cybersecurity.
- GFCE & KPMG. (2023). 'African Cybersecurity Capacity Review 2023.' *Global Forum on Cyber Expertise*.
- Gupta, D., Elluri, L., Jain, A., Moni, S. S., & Aslan, O. (2024). 'Blockchain-enhanced frameworks for secure third-party vendor risk management.' *Journal of Information Security and Applications*, 75, 103657.
- Iltter, I. (2024). Third-party cybersecurity risk. *Journal of Risk and Financial Management*, 17(2), 78.
- ISO/IEC 27001, (2022). *Information Security Management Systems — Requirements*. International Organization for Standardization.
- Kerzner, H. (2019). *Project management: A systems approach* (12th ed.). Wiley.
- Kombo, D.K. and Tromp, D.L.A. (2006). *Proposal and thesis writing: an introduction*. Nairobi: Paulines Publications Africa
- Kshetri, N. (2019). Cybersecurity economics. *Telecommunications Policy*, 43(6), 101814.
- Moltke, H., & Xu, J. (2022). Cyber incidents and project disruption. *Information Systems Frontiers*, 24(3), 567–583.
- Mwila, T. (2020). 'Cybersecurity readiness in Zambia's telecommunications sector.' *Zambia ICT Research Journal*, 4(1), 21–33.
- Ncube, L., & Ngulube, P. (2022). 'Cybersecurity readiness of ICT vendors in Southern Africa: Challenges and prospects.' *Southern African Journal of Information and Communication*, 24(1), pp. 22–37.
- NIST (2020). *Cybersecurity Framework Version 1.1*. National Institute of Standards and Technology, U.S. Washington: Department of Commerce.
- Project Management Institute (PMI). (2021). *A guide to the project management body of knowledge (PMBOK® Guide)* (7th ed.). Project Management Institute.
- PwC. (2025). *Global Digital Trust Insights: 2025*. PricewaterhouseCoopers.

Sarantakos, S. (1998). *Social research*. (2nd Ed.). Southern Melbourne: MacMillan Education.

Savunen, P. (2024). 'The impact of cyber threats on project implementation timelines in ICT industries.' *Project Management Journal*, 55(3), 201–215.

Sharma, R. & Chen, Y. (2021). 'Supply chain cybersecurity risks in telecommunications: Emerging challenges and mitigation strategies.' *Journal of Cybersecurity*, 7(2), pp.1–17.

Suzuki, T. (2020). 'Reputational damage from cyber incidents: The hidden cost for digital enterprises.' *Journal of Cyber Policy*, 5(3), 310–329.

Wang, Y., Ho, K., & Shan, S. (2024). 'Cybersecurity risk and firm innovation: Evidence from international data.' *Journal of Business Research*, 172, pp. 114–129.

Zambia Information and Communications Technology Authority (ZICTA). (2023). *Annual ICT Sector Performance Report*. Lusaka: ZICTA.

