International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Operational Technology Cybersecurity Resilience Framework for Zimbabwe's Mining Sector: Integrating Threat Intelligence and Contextual Risk Mitigation Strategies

Jairos Mukwenha

Zimbabwe Open University: Cnr Leopard Takawira and Samora Machel Avenue, Harare, ZW

ABSTRACT

The increasing digital transformation within critical infrastructure sectors globally presents significant cybersecurity challenges, particularly for Operational Technology (OT) systems. This paper proposes a comprehensive cybersecurity resilience framework specifically tailored for Zimbabwe's mining sector, a vital economic pillar heavily reliant on OT. The framework integrates proactive threat intelligence with adaptive, contextual risk mitigation strategies to enhance the sector's ability to withstand, detect, and recover from cyberattacks. It addresses unique challenges such as legacy systems, skill shortages, and remote operations prevalent in the Zimbabwean context. Through a four-phase approach encompassing assessment, threat intelligence integration, contextual risk mitigation, and continuous improvement, this framework aims to establish a robust and adaptive cybersecurity posture, safeguarding operational continuity, safety, and economic stability

Keywords: Operational Technology, Mining Cybersecurity, Critical Infrastructure, Zimbabwe, Resilience Framework, Threat Intelligence

1. INTRODUCTION AND BACKGROUND

The global mining industry, particularly in Zimbabwe, is undergoing a technological transformation marked by the integration of advanced OT systems that enhance extraction, processing, and logistics operations. The Zimbabwean mining sector has historically been a mainstay of the national economy, and its dependency on sophisticated OT environments is escalating (Jörgensen & Mikkelsplass, 2023). As the industry embraces increased digitisation and the convergence of Information Technology (IT) and OT networks, cybersecurity concerns emerge because this amalgamation expands the potential attack surface, making critical processes vulnerable to advanced cyber threats (Slimane, 2024).

Within the context of Zimbabwe, the mining industry's obstacles are compounded by several factors, including outdated legacy systems, limited oversight of industrial networks, a shortage of specialised cybersecurity personnel, financial constraints, and the geographic isolation typical of mining operations (Matthiesen & Bjørn, 2015; Roldán et al., 2019). Cyberattacks targeting OT infrastructure in mines may lead not only to severe operational disruptions but can also compromise safety protocols, cause environmental harm, and incur significant financial losses, alongside damaging reputational impacts (Slimane, 2024).

To address these multifaceted challenges, this paper presents a cybersecurity resilience framework tailored to OT in Zimbabwe's mining industry. This framework stands out by focusing on the proactive integration of dynamic threat intelligence with nuanced risk mitigation strategies contextualised to the specific scenarios faced by the industry (Arora et al., 2022). The primary objective of this research is to provide a structured methodology that empowers Zimbabwean mining enterprises to build, strengthen, and continuously enhance their cybersecurity posture, ensuring the industry's resilience and long-term viability amidst evolving technological demands (Dave, 2023).

The framework aims to foster a culture of security that acknowledges the sector's specific vulnerabilities while adapting to the broader trends in digital transformation driven by the convergence of IT and OT. By leveraging contemporary security practices and emphasising continuous improvement, the mining sector in Zimbabwe can navigate its complex landscape more effectively and maintain its crucial role in the national economy.

2. LITERATURE REVIEW

The necessity for robust cybersecurity measures in critical infrastructure, particularly within the domain of OT, has garnered substantial attention from both academia and the industry. According to the National Institute of Standards and Technology (NIST), OT systems are essential for the management of industrial networks, where safety, availability, and integrity are paramount, often overshadowing the traditional IT focus on confidentiality (Adegbite et al., 2023). This distinction is critical as OT environments are increasingly targeted due to their integration within the broader context of Industry 4.0, where the convergence of IT and OT introduces new vulnerabilities through interconnected industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems (Abrahams et al., 2024). The evolution of cyber threats necessitates a paradigm shift, placing significant emphasis on understanding the specific operational challenges encountered in these environments.

Existing cybersecurity frameworks provide a foundational approach to managing risks associated with these unique systems. The NIST Cybersecurity Framework (CSF) presents a versatile structure for organisations, advocating a holistic view of cybersecurity through the phases of identification, protection, detection, response, and recovery (Adegbite et al., 2023). Similarly, the ISA/IEC 62443 standards offer comprehensive best practices tailored to the needs of industrial automation and control systems (IACS), addressing both technical requirements and organisational policies (Abrahams et al., 2024). However, applying these frameworks in the context of developing nations, such as Zimbabwe, necessitates adaptations that consider the local operational, economic, and regulatory landscapes (Balisane et al., 2024).

Research has shown that the mining sector in Zimbabwe faces multifaceted challenges, including the widespread presence of legacy systems that were designed without modern cybersecurity considerations, thus exposing critical vulnerabilities (Curran et al., 2024; Gochero, 2018). Additionally, the acute shortage of skilled cybersecurity professionals with expertise in both IT and OT sectors compounds these challenges, significantly hindering the sector's ability to bolster its defences (Olaniran, 2024b). Coupled with limited financial resources for investing in advanced security measures, organisations are often compelled to prioritise essential operational costs over security upgrades (Olaniran, 2024a). The geographic isolation of many mining operations further complicates physical security and incident response capabilities, necessitating innovative approaches to maintain protection in remote locations (Bodemer, 2023).

Given the evolving threat landscape characterised by state-sponsored attacks and sophisticated ransomware campaigns, the integration of threat intelligence into cybersecurity frameworks has been recognised as essential for preemptive defence strategies (Obiki-Osafiele et al., 2024). Effective threat intelligence encompasses insights on adversaries' tactics, techniques, and procedures (TTPs), as well as indicators of compromise (IoCs), enabling organisations to tailor their defences against specific threats (Atanasov, 2024). However, simply obtaining threat intelligence is inadequate; it necessitates contextualisation and actionable insights relevant to an organisation's specific operational conditions (Udeh et al., 2024).

In response to these critical concerns, this paper aims to establish a comprehensive, contextualised cybersecurity framework for the Zimbabwean mining sector. By synthesising established cybersecurity principles with the unique challenges faced in this critical industry, this research emphasises the synergistic combination of threat intelligence and tailored risk mitigation strategies to enhance resilience against emerging cyber threats.

3. MATERIALS AND METHODS

This research proposes an OT cybersecurity resilience framework designed for Zimbabwe's mining sector. The methodology for developing this framework involved a synthesis of established cybersecurity best practices such as NIST CSF, ISA/IEC 62443, an analysis of unique challenges within the Zimbabwean mining context, and an emphasis on the synergistic integration of threat intelligence and contextual risk mitigation. The framework is structured into four interconnected phases, each comprising specific objectives and methodologies, presented as the components of this resilience strategy.

3.1. Framework Structure

The proposed framework is modular and iterative, consisting of the following phases as given in Figure 1.

Figure 1: Operational Technology Cybersecurity Resilience Framework

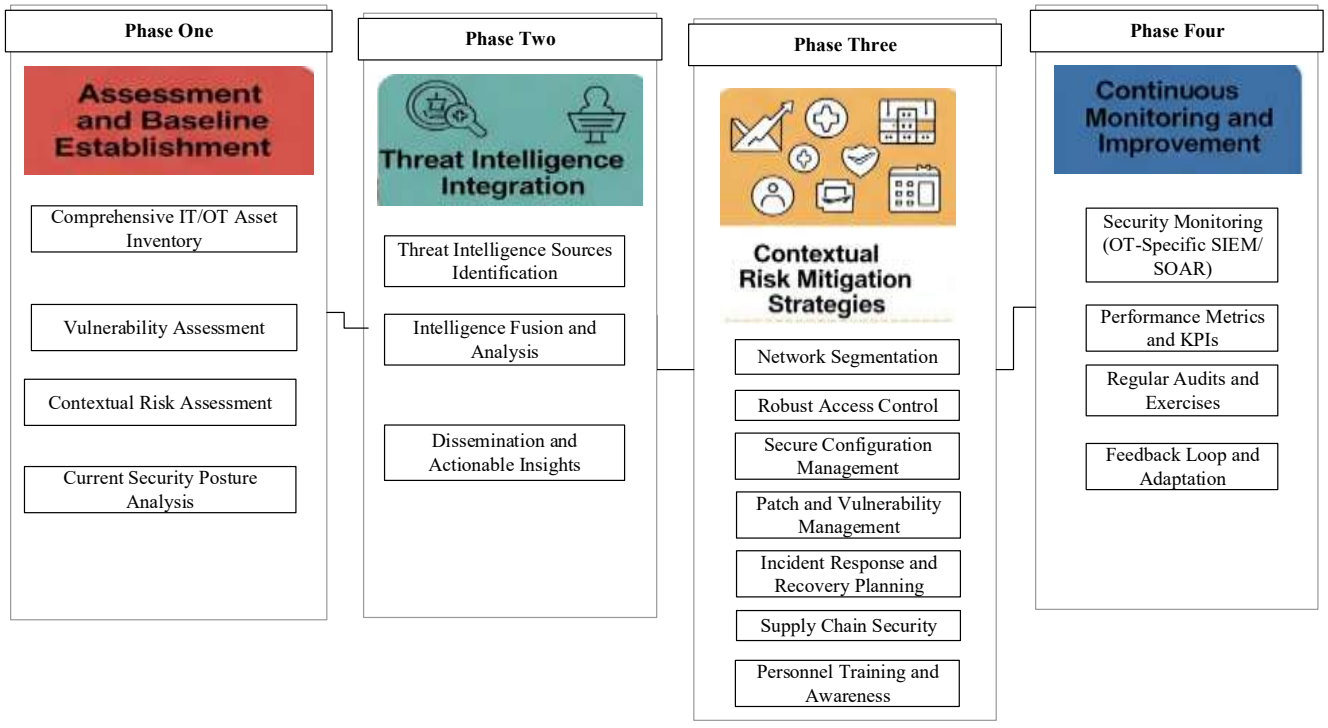

Figure 1 shows the framework's design, which is informed by a critical assessment of the Zimbabwean mining context, as described in the introduction and literature review, ensuring that mitigation strategies are not generic but specifically address local constraints and operational realities.

4. Results and Discussion

The proposed OT Cybersecurity Resilience Framework, when implemented within Zimbabwe's mining sector, is expected to yield significant improvements in cybersecurity posture and operational continuity. The results are presented as the anticipated outcomes and benefits derived from the framework's structured application, followed by a discussion of how its core tenets address the sector's specific challenges and integrate threat intelligence effectively.

4.1. Anticipated Results of Framework Implementation

The initial phase of the framework, which focuses on assessment and baseline establishment, facilitates a thorough inventory of all IT and OT assets. This enhanced visibility allows organisations to identify their attack surface more clearly and prioritise their security defences accordingly. Such proactive asset management shifts the paradigm from reactive to proactive security measures (Holasova et al., 2024). By integrating threat intelligence in the second phase of the framework, mining operations develop the ability to foresee emerging vulnerabilities and threats tailored to their specific OT systems. This proactive anticipation minimises reaction times and enables pre-emptive defences, significantly decreasing the chances of successful cyberattacks.

The third phase, which involves contextual risk mitigation, ensures the implementation of security controls that are not generic but tailored to each mining site's unique operational processes, threat landscapes, and risk tolerances. By aligning security measures with specific needs, resources can be optimised for maximum effectiveness in reducing risk to critical functions (Nobles, 2018). The structured planning and regular testing outlined in Phase 3 result in clearer roles, defined procedures, and faster recovery times in the event of a cyber incident, minimising operational downtime and associated financial losses. By systematically vetting vendors and monitoring third-party access (Phase three), the framework significantly reduces the risk of supply chain attacks, a growing concern for critical infrastructure.

The Phase three's emphasis on personnel training and awareness is expected to foster a heightened sense of cybersecurity responsibility among employees, transforming human vigilance into a critical layer of defence against both external and insider threats. The final phase promotes continuous monitoring and improvement, creating an iterative feedback loop that adapts the organisation's cybersecurity posture to evolving threats. This flexibility is crucial for maintaining resilience in a rapidly changing cyber landscape (Progoulakis et al., 2021).

4.2. Discussion: Addressing Challenges and Integration Effectiveness

The framework is tailored to confront the unique cybersecurity challenges within Zimbabwe's mining sector effectively. For example, while many legacy OT systems might be resistant to direct updates, the framework encourages implementing compensating controls, such as network segmentation and robust access control measures. This is particularly vital for identifying exploits that may target these older systems, allowing for strategic virtual patching when necessary. To tackle limited visibility, the comprehensive asset inventory established in the first phase, combined with ongoing monitoring from phase four, ensures consistent visibility across OT environments. By establishing a baseline and maintaining surveillance, organisations can keep abreast of their security posture.

A critical factor in enhancing the cybersecurity landscape is the skill shortage present in many developing

nations. Recognising this, the framework focuses on personnel training as a strategic initiative aimed at upskilling existing staff and fostering a culture of cyber vigilance. Targeting a skilled workforce can be supplemented through strategic partnerships and collaborations that extend capabilities. Given that budgetary constraints often impact investment in cybersecurity, the framework's approach to contextual risk mitigation allows for judicious allocation of limited resources. By directing investment towards areas deemed high-impact, organisations can achieve worthwhile security enhancements without straining budgets excessively.

The emphasis on robust access control mechanisms, secure network designs, and well-structured incident response plans specifically addresses the intricacies of securing remote operations in the mining industry, a context further complicated by geographic dispersion. To mitigate insider threats, the framework prescribes stringent access controls, continuous monitoring capabilities, and robust security awareness programs. This comprehensive configuration aims to safeguard OT systems against both intentional and unintentional insider risks. The integration of threat intelligence into the framework is its cornerstone, promoting proactive defence measures. As threats evolve, the obtained intelligence informs the risk assessment process, allowing for accurate evaluations that lead to proactive defence strategies rather than mere reactive ones.

Furthermore, the framework establishes a dynamic model for targeted risk mitigation, ensuring that if intelligence signals a potential vulnerability in a specific system, the appropriate countermeasures for that specific scenario are prioritised. This focused approach stands in contrast to traditional strategies that may apply updates uniformly without a nuanced understanding of operational importance. By intertwining threat intelligence with real-time security monitoring, the framework enables rapid detection and response to emerging threats, thereby enhancing overall situational awareness. Most importantly, it allows organisations to optimise their cybersecurity investments, ensuring that resources are effectively utilised against the most pressing threats.

The OT Cybersecurity Resilience Framework represents a shift towards a risk-informed, intelligence-driven strategy tailored specifically for the Zimbabwean mining sector. This framework not only positions companies to contend with current cyber threats but equips them to adapt to future challenges, subsequently reinforcing the sector's operational stability and the national economy's security.

Conclusion

The increasing interconnectivity of Operational Technology (OT) systems within Zimbabwe's vital mining sector necessitates a robust and adaptive cybersecurity strategy. This paper has presented a comprehensive OT cybersecurity resilience framework designed to address the unique challenges faced by the industry, including legacy systems, skill shortages, budgetary constraints, and remote operations. By systematically progressing through four interconnected phases—Assessment and Baseline Establishment, Threat Intelligence Integration, Contextual Risk Mitigation Strategies, and Continuous Monitoring and Improvement—the framework provides a structured approach to building and maintaining a resilient cybersecurity posture.

The core strength of the proposed framework lies in its emphasis on the tight integration of actionable threat intelligence with highly contextualised risk mitigation. This synergistic approach enables mining operations to move from reactive defence to proactive threat anticipation, ensuring that security investments are targeted effectively where they yield the greatest protective benefit. By understanding specific threats to their unique operational environments, Zimbabwean mines can implement precise

controls, enhance incident response capabilities, and significantly reduce the likelihood and impact of cyberattacks.

Successful implementation of this framework is critical for safeguarding operational continuity, ensuring worker safety, protecting environmental integrity, and preserving the economic contribution of Zimbabwe's mining industry. It underscores the imperative for recognising cybersecurity as a strategic investment rather than a mere IT overhead. The proposed framework serves as a vital blueprint for enhancing OT cybersecurity resilience, ensuring the long-term sustainability and digital security of Zimbabwe's critical mining sector

The researcher recommends future research on empirically validating this framework through pilot implementations in various Zimbabwean mining operations, collecting quantitative and qualitative data on its effectiveness, usability, and return on investment.

In addition, there should be an investigation into the specific regulatory and policy mechanisms required to support the widespread adoption and enforcement of such a framework within the Zimbabwean legal and industrial context.

References

1. Abrahams, T. O., Ewuga, S. K., Dawodu, S. O., Adegbite, A. O., & Hassan, A. O. (2024). A REVIEW OF CYBERSECURITY STRATEGIES IN MODERN ORGANIZATIONS: EXAMINING THE EVOLUTION AND EFFECTIVENESS OF CYBERSECURITY MEASURES FOR DATA PROTECTION. *Computer Science & IT Research Journal*, *5*(1), 1–25. https://doi.org/10.51594/csitrj.v5i1.699
2. Adegbite, A. O., Akinwolemiwa, D. I., Uwaoma, P. U., Kaggwa, S., Akindote, O. J., & Dawodu, S. O. (2023). REVIEW OF CYBERSECURITY STRATEGIES IN PROTECTING NATIONAL INFRASTRUCTURE: PERSPECTIVES FROM THE USA. *Computer Science & IT Research Journal*, *4*(3), 200–219. https://doi.org/10.51594/csitrj.v4i3.658
3. Arora, A., Wright, V., & Garman, C. (2022). Strengthening the Security of Operational Technology: Understanding Contemporary Bill of Materials. *Journal of Critical Infrastructure Policy*, *3*(1), 111–135. https://doi.org/10.18278/jcip.3.1.8
4. Atanasov, I. (2024). From Firewall to AI: Strengthening Linux Server Security. *Science, Engineering and Education*, *9*(1), 3–12. https://doi.org/10.59957/see.v9.i1.2024.1
5. Balisane, H., Egho-Promise, E. I., Lyada, E., & Aina, F. (2024). TOWARDS IMPROVED THREAT MITIGATION IN DIGITAL ENVIRONMENTS: A COMPREHENSIVE FRAMEWORK FOR CYBERSECURITY ENHANCEMENT. *International Journal of Research -GRANTHAALAYAH*, *12*(5). https://doi.org/10.29121/granthaalayah.v12.i5.2024.5655
6. Bodemer, O. (2023). The Unseen Guardian: How Blockchain, Java, and AI Stealthily Became the Sherlock Holmes of Cybersecurity. *Engineering: Open Access*, *1*(3). https://doi.org/10.33140/EOA.01.03.08
7. Curran, K., Curran, E., Killen, J., & Duffy, C. (2024). The role of generative AI in cyber security. *Metaverse*, *5*(2), 2796. https://doi.org/10.54517/m2796
8. Gochero, P. (2018). Econometric Analysis of Foreign Direct Investment in the Zimbabwean Mining Sector 2005-2014. *Theoretical Economics Letters*, *08*(14), 3157–3177. https://doi.org/10.4236/tel.2018.814196

9. Holasova, E., Fujdiak, R., & Misurec, J. (2024). Comparative Analysis of Classification Methods and Suitable Datasets for Protocol Recognition in Operational Technologies. *Algorithms*, *17*(5), 208. https://doi.org/10.3390/a17050208
10. Slimane, J. Ben. (2024). Securing the Industrial Backbone: Cybersecurity Threats, Vulnerabilities, and Mitigation Strategies in Control and Automation Systems. *Journal of Electrical Systems*, *20*(7s), 1111–1120. https://doi.org/10.52783/jes.3604
11. Jörgensen, P.-A., & Mikkelsplass, S. A. (2023). Creating a Testbed for Cyber Security Assessment of Industrial 4.0 Factory Infrastructure. *Proceeding of the 33rd European Safety and Reliability Conference*, 3374–3381. https://doi.org/10.3850/978-981-18-8071-1_P532-cd
12. Matthiesen, S., & Bjørn, P. (2015). Why Replacing Legacy Systems Is So Hard in Global Software Development. *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, 876–890. https://doi.org/10.1145/2675133.2675232
13. Nobles, C. (2018). Botching Human Factors in Cybersecurity in Business Organizations. *HOLISTICA – Journal of Business and Public Administration*, *9*(3), 71–88. https://doi.org/10.2478/hjbpa-2018-0024
14. Obiki-Osafiele, A. N., Agu, E. E., & Chiekezie, N. R. (2024). Protecting digital assets in Fintech: Essential cybersecurity measures and best practices. *Computer Science & IT Research Journal*, *5*(8), 1884–1896. https://doi.org/10.51594/csitrj.v5i8.1449
15. Olaniran, O. T. (2024a). The Role of Explainable AI in Enhancing Threat Intelligence Analysis in Cybersecurity Operations. *International Research Journal of Modernization in Engineering Technology and Science*. https://doi.org/10.56726/IRJMETS60971
16. Olaniran, O. T. (2024b). User Satisfaction and Trust of AI Explanations in Threat Intelligence Analysis: Implications for Acceptance and Usability. *International Research Journal of Modernization in Engineering Technology and Science*. https://doi.org/10.56726/IRJMETS60972
17. Progoulakis, I., Rohmeyer, P., & Nikitakos, N. (2021). Cyber Physical Systems Security for Maritime Assets. *Journal of Marine Science and Engineering*, *9*(12), 1384. https://doi.org/10.3390/jmse9121384
18. Dave, D. M. K. (2023). Revolutionizing Manufacturing: The Pivotal Role of Artificial Intelligence in Software-Defined Processes. *International Research Journal of Modernization in Engineering Technology and Science*. https://doi.org/10.56726/IRJMETS47054
19. Roldán, J. J., Crespo, E., Martín-Barrio, A., Peña-Tapia, E., & Barrientos, A. (2019). A training system for Industry 4.0 operators in complex assemblies based on virtual reality and process mining. *Robotics and Computer-Integrated Manufacturing*, *59*, 305–316. https://doi.org/10.1016/j.rcim.2019.05.004
20. Udeh, E. O., Amajuoyi, P., Adeusi, K. B., & Scott, A. O. (2024). The integration of artificial intelligence in cybersecurity measures for sustainable finance platforms: An analysis. *Computer Science & IT Research Journal*, *5*(6), 1221–1246. https://doi.org/10.51594/csitrj.v5i6.1195