Sixth International Conference in Information and Communication Technologies, Lusaka, Zambia
15th to 16th October 2024

Advancing Cybersecurity Measures to Safeguard Critical Infrastructure and Data: Is Zambia Ready?

Christine Simfukwe
Natural Sciences and Mathematics
Copperbelt University,
Kitwe, Zambia,
cmsimfukwe@gmail.com

Dr. Alice P Shemi,
Natural Sciences and Mathematics
Copperbelt University

Kitwe, Zambia

shemiap@gmail.com

Abstract— As digital technologies become increasingly integral to critical infrastructure, emerging economies like Zambia are facing heightened cybersecurity threats. Current security measures are often inadequate, leaving essential services vulnerable to potential cyber-attacks. This research aims to develop a comprehensive cybersecurity framework tailored to safeguarding Zambia's critical infrastructure and data. By identifying existing vulnerabilities and proposing innovative solutions, the study seeks to enhance the resilience of Zambia's critical infrastructure against cyber threats. The focus will be on practical tools and software to strengthen national security, ensure economic stability, and protect sensitive data. The findings will contribute to a stronger cybersecurity posture for Zambia, addressing the unique challenges faced by emerging economies in the digital era.

Keywords—Cybersecurity, Critical Infrastructure, Emerging Economies, Cyber Threats, Security Framework

I. INTRODUCTION

This research aims to enhance current digital security frameworks by incorporation of best practices and technologies tailored to protect critical infrastructure and data in emerging economies, focusing on Zambia. The study will investigate existing vulnerabilities, propose innovative security solutions, and implement these solutions through the development of practical tools and software. The goal is to enhance the resilience of Zambia's critical infrastructure against cyber threats and ensure the protection of sensitive data.

Background and Significance

With the increasing reliance on digital technologies, critical infrastructure in emerging economies like Zambia faces growing cybersecurity threats. The existing security measures are often inadequate, leaving essential services vulnerable to cyber-attacks. Enhancing cybersecurity frameworks to protect critical infrastructure is crucial for national security, economic stability, and the safety of sensitive data. To address the growing threat of cyber-attacks on critical infrastructure, organizations worldwide adopt various cybersecurity frameworks to guide their security strategies and ensure compliance with best practices

A. Problem Statement

In recent years, Zambia has seen an increase in cybercrime as bad actors exploit its's critical infrastructure in sectors such as energy, healthcare, education, and finance. With the growing reliance on digital technologies and the increased handling of personal data, cybersecurity has become a cornerstone of data protection worldwide. In 2021, The Zambia Computer Incident Response Team (ZM-CIRT) recorded over 10 million cyberattacks targeted at Zambian citizens and businesses leading to 50,000 investigations, a number that doubled to 100,000 by 2022 [1].

In response to the vulnerability to sophisticated cyber threats, the government has begun to combat this issue, by implementing the 2021 Cyber Security and Cyber Crimes Act No. 2, which established a system for addressing cyber incidents and guiding policy to protect citizens' data [2]. Despite these efforts, a 2023 study by Liquid Intelligence Technologies revealed a rise in cybercrime, particularly among new internet users who lack awareness of potential scams [1]. This heightened risk is part of a broader trend, such as the sophisticated internet fraud syndicate that was uncovered, leading to the arrest of 77 people, including 22 Chinese nationals in 2023. A company registered as Golden Top Support Services presented itself as a normal call center. In fact, it was a Chinese-owned cybercrime operation using WhatsApp, Telegram and other communication platforms to scam people out of their money.

Common cybercrimes include monetary and wholesale fraud, extortion, mobile money reversal scams, social media account hijacking, and fake online product promotions. To address these threats, Zambia has taken several steps to strengthen its cybersecurity efforts. Zambia has established regulatory and enforcement bodies such as the Zambia Information and Communications Technology Authority (ZICTA) and the Zambia Police Service's Cybersecurity and Cybercrime Unit. These organizations oversee the

 ISBN: 978-9982-95-500-3

cybersecurity landscape with the aim of reducing cyber risks across various sectors. Additionally, Zambia has strengthened its international partnerships through multilateral agreements to facilitate information sharing and cross-border collaboration on cybersecurity. Recognizing the importance of education in combating cyber threats, the country has invested in training and public awareness initiatives, which target professionals, youth, and the general public to build resilience against cyber risks. Further, the launch of the Cyber Security Fusion Centre provides Zambian stakeholders with real-time, intelligence-driven alerts and advisory services to safeguard against cybercrime. According to Siampondo and Chansa [1], despite the progress made by agencies like the Zambia Information and Communications Technology Authority and the Cybersecurity and Cybercrime Unit, the overall fight against cybercrime remains underfunded and understaffed. They call for an updated legal framework to address evolving threats and emphasize the importance of public-private partnerships in enhancing cybersecurity resilience. This situation highlights the pressing need for a resilient, context-specific cybersecurity framework that can address vulnerabilities across critical infrastructure sectors and adapt to the evolving threat landscape.

B. Research Questions

1) What are the primary cybersecurity vulnerabilities and threats facing Zambia's critical infrastructure?
2) What are the existing cybersecurity frameworks used to protect Zambia's critical infrastructure and sensitive data?
3) How can new cybersecurity measures and tools developed help to strengthen the resilience of Zambia's critical infrastructure?
4) How can the effectiveness of these developed tools be evaluated and validated in real-world scenarios?

I. LITERATURE REVIEW

As digital transformation accelerates worldwide, the internet has become the backbone of service delivery, seamlessly connecting organizations across all sectors. This interconnected network manages sensitive data such as financial records, personal information, and national security assets, making it an increasingly attractive target for cybercriminals

C. Cybersecurity Legislation in Zambia

In Zambia, the Data Protection Act [3] provides a foundational legal framework to safeguard personal information. As Kizza [4] points out, effective cybersecurity is crucial for compliance with regulations and for preventing potential cyber-attacks on critical infrastructure. However, this legislation alone cannot ensure adequate protection without complementary cybersecurity measures.

The Cyber Security and Cyber Crimes Act [5] is a key legislative tool that outlines the identification and protection of critical information infrastructure. The Act defines "critical information" as data deemed essential for national security and socio-economic well-being, and "critical information infrastructure" as the cyber infrastructure necessary for public safety, economic stability, and national security . Despite this legislation, cybersecurity implementation remains inconsistent across sectors.

D. Cybersecurity Challenges

As Solms and Niekerk [6] note, cybersecurity measures are essential to safeguard networks, systems, and data from cyber-attacks. Yet, many Zambian organizations face challenges in implementing adequate cybersecurity strategies. Mulenga [7] highlights that many institutions struggle with compliance due to limited cybersecurity infrastructure, leaving vital systems exposed. This is echoed by Mansfield-Devine [8] who emphasizes that the lack of investment in cybersecurity increases vulnerability to attacks such as data breaches and ransomware.

E. Gaps in Awareness and Training

Phiri [9] argues that a lack of awareness and resources has hindered the full adoption of the Cyber Security and Cyber Crimes Act. Many organizations fail to provide adequate training, leaving employees unprepared for potential cyber threats. Manyika [10] calls for stronger regulatory oversight and more extensive training programs to address these gaps, ensuring that all sectors can meet the challenges posed by cyber risks.

II. METHODOLOGY

This research will adopt a mixed-methods approach, integrating both qualitative and quantitative techniques to comprehensively address the complex nature of cybersecurity within Zambia's critical infrastructure. Mixed-methods research has been shown to be particularly effective for investigating multifaceted issues like cybersecurity, as it allows for both in-depth exploration and robust validation [11]. Initially, qualitative methods, including expert interviews and thematic analysis, will be employed to identify and analyse key cybersecurity vulnerabilities, threats, and current mitigation practices [12]. This qualitative insight will then be supplemented by quantitative data collection through surveys, statistical analysis, and potentially machine learning-driven anomaly detection, to further elucidate the scope and prevalence of these vulnerabilities [13]. A comprehensive review of existing digital security frameworks, global best practices, and

 ISBN: 978-9982-95-500-3

cybersecurity technologies will inform the development of a customized cybersecurity framework drawing on established guidelines and best practices. Advancements in artificial intelligence, especially in automated threat detection and real-time risk assessment, are under consideration to enhance the framework's adaptability and scalability [14]. Finally, the framework's effectiveness will be validated through pilot implementations and testing in selected real-world environments, using quantitative metrics like threat detection rates, response times, and resilience scores, while qualitative feedback from stakeholders will capture user experiences and implementation challenges [15].

This combined approach ensures a comprehensive analysis of Zambia's cybersecurity landscape and supports the development and validation of an adaptable, effective cybersecurity solution for critical infrastructure

III. SURVEY RESULTS

A survey conducted for this study reveals a sectoral imbalance in cybersecurity preparedness. The Energy/Utilities sector had the largest representation (29.4%), followed by Healthcare (20.6%), and both Higher Education and Telecommunications at 14.7%. Notably, the Government/Public Sector accounted for 8.8%, while None Governmental Organisations (NGOs) and other sectors had no representation. These results indicate a focus on sectors with significant exposure to cybersecurity risks. Respondents were predominantly ICT Managers/Directors or IT Support Staff, with a small number of Cybersecurity Specialists and Academic Faculty. ICT Managers generally demonstrated a stronger grasp of organizational cybersecurity policies than IT Support Staff, highlighting a potential knowledge gap at the operational level.

A. Cybersecurity Awareness and Practices

The survey showed that cybersecurity awareness varies widely across organizations. The majority (35.3%) rated their cybersecurity awareness as moderate, with 32.4% rating it as very high. Only 5.9% rated their awareness as very low, indicating a wide disparity in preparedness.

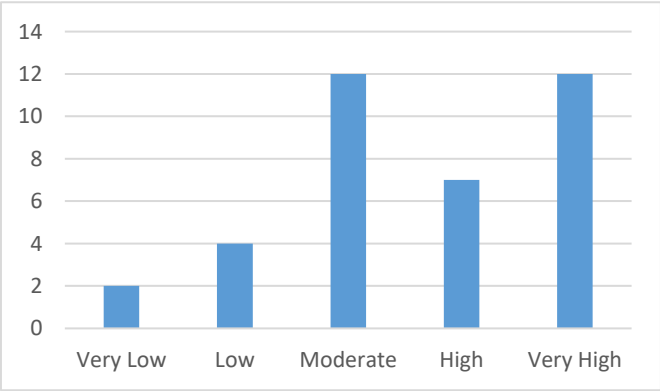

Fig 1: Rate of Cybersecurity Awareness

A notable 70.6% of organizations reported having formal cybersecurity policies, signaling a commitment to structured practices as shown in figure 1. However, 29.4% either lacked policies or were unaware of their existence, reflecting potential gaps in communication or policy formulation.

The lack of cybersecurity training was evident as shown in Figure 2, with 27% of organizations not conducting any form of training—a critical area for improvement.

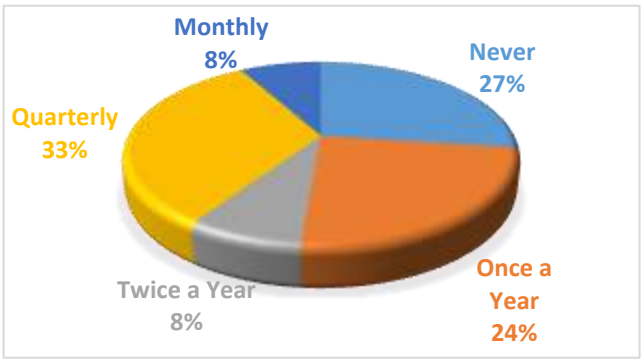

Fig 2: Cybersecurity User Training

B. Cybersecurity Threats and Challenges

Phishing attacks and lack of employee awareness emerged as the top concerns, each cited by 55.9% of respondents. The absence of frequent training correlates directly with the perception of inadequate employee preparedness. Other significant threats included ransomware (41.2%) and insider threats (32.4%). Despite this, only 26.5% of respondents felt moderately confident in handling cybersecurity incidents, underscoring the need for stronger response mechanisms.

C. Recommendations

Training and Awareness: To improve Zambia's cybersecurity landscape, a concerted effort must be made to increase employee training and awareness. With 64.7% of respondents identifying this as a key area of need, it is clear that investment in training will significantly mitigate risks like phishing and insider threats.

Technological Investments: Organizations recommended a range of cybersecurity tools, including firewalls, SIEM (Security Information and Event Management) systems, and intrusion detection/prevention systems. These tools are essential for protecting critical infrastructure and reducing exposure to cyber-attacks.

Government Support: Survey participants strongly called for increased government support, particularly in training, policy formulation, and public awareness campaigns. Barriers such as limited budgets, a lack of skilled personnel, and insufficient executive support were identified as obstacles to implementing effective cybersecurity strategies.

 ISBN: 978-9982-95-500-3

Collaboration between institutions and the government is critical for improving the country's overall cybersecurity posture.

IV. CONCLUSION

Zambia's cybersecurity readiness, while improving, faces substantial challenges in areas such as training, funding, and executive support. Although legislative frameworks like the Cyber Security and Cyber Crimes Act and the Data Protection Act provide a solid foundation, their enforcement and application remain uneven. As digital transformation continues, there is a clear need for enhanced, coordinated efforts between the government and private sectors to safeguard critical infrastructure and data in Zambia.

V. ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to Dr. Alice P. Shemi for her invaluable guidance and mentorship throughout the development of this paper. I am equally thankful to my colleagues, peers, and family, whose encouragement and insights have been a source of inspiration during this journey. Lastly, I acknowledge the broader academic and professional communities whose work laid the foundation for this research.

References

[1] Siampondo, G. M., Sumbwanyambe, M., & Chansa, B. (2022). A study on the existing cybersecurity policies and strategies in combating increased cybercrime in Zambia. Journal of Information Security, 14(4), 294-303. https://doi.org/10.4236/jis.2023.144017

[2] Mwila, A. K. (2021). Cybersecurity challenges in Zambia: A call for action. LinkedIn. Retrieved from https://www.linkedin.com

[3] Republic of Zambia, 2021. Data Protection Act, 2021. Lusaka: Government of Zambia. Available at: https://www.parliament.gov.zm/node/8853# [Accessed 24 Sept. 2024].

[4] Kizza, J.M., 2021. Guide to computer network security. 4th ed. Cham: Springer.

[5] Republic of Zambia, 2021. The Cyber Security and Cyber Crimes Act, Act No. N.A.B. 2 of 2021. Lusaka: Government of Zambia. Available at: https://www.parliament.gov.zm/sites/default/files/documents/acts/Act%20No.%202%20of%202021%20The%20Cyber%20Security%20and%20Cyber%20Crimes.pdf [Accessed 24 Sept. 2024].

[6] Solms, R. and Niekerk, J., 2013. From information security to cyber security. Computers & Security, 38, pp.97-102

[7] Mulenga, P., 2022. Implementation of the Zambia Data Protection Act: Challenges and opportunities. African Journal of Information Security, 4(2), pp.12-24.

[8] Mansfield-Devine, S., 2016. Ransomware: Taking businesses hostage. Network Security, 2016(10), pp.8-17.

[9] Phiri, M., 2020. The state of cybersecurity in Zambia: Policy, practice, and perceptions. Cybersecurity Journal of Southern Africa, 10(3), pp.34-51.

[10] Manyika, T., 2021. Cybersecurity readiness in Zambia: An evaluation of legal frameworks and technological advancements. Zambia Journal of Law and Technology, 12(1), pp.45-56.

[11] Creswell, J. W., & Clark, V. L. P. (2021). Designing and conducting mixed methods research (4th ed.). SAGE Publications

[12] Venkatesh, V., Brown, S. A., & Bala, H. (2020). Guidelines for conducting mixed methods research in information systems. MIS Quarterly, 44(2), 455-478.

[13] Yin, R. K. (2021). Case study research and applications: Design and methods (7th ed.). SAGE Publications.

[14] Sharma, R., Kaushal, R., & Gupta, A. (2023). Cybersecurity AI systems: Advances and challenges in implementation. Cybersecurity in Intelligent Systems, 8(3), 221-238.

[15] Patton, M. Q. (2022). Qualitative research & evaluation methods (5th ed.). SAGE Publications.