

Evaluation of a Cyber Security Resilience as a Factor for Regulating Critical Infrastructure

Grenah Sivwimi*, Simon Tembo

Department of Electrical & Electronic Engineering, School of Engineering, University of Zambia, Lusaka, Zambia

Abstract This research explores the role of Cyber Security Resilience in regulating Critical Infrastructure in Zambia, focusing on Zambia Information Communication Technology Authority, (ZICTA) Airtel, MTN, Zambian National Commercial Bank (ZANACO), National Airport Corporation, Zambia Police Service, Drug Enforcement Commission, Information Communications Technology Association of Zambia, University of Zambia, Mulungushi University, Copperbelt University (CBU) and Zambia Centre for Accountancy Studies in Zambia. Employing a case study approach and utilizing questionnaires, data was collected to investigate the awareness, effectiveness, challenges, and prevalent forms of cyber-attacks on critical infrastructure. The findings highlight a significant awareness of existing cybersecurity strategies but a perceived ineffectiveness in addressing cyber threats. Challenges identified include limited technical expertise, lack of collaboration, rapidly evolving threats, and budget constraints. Phishing attacks emerged as the most prevalent form of cyber-attacks, underscoring the need for targeted strategies. Respondents emphasized the necessity for a comprehensive framework and prioritized regular cybersecurity audits and assessments. Recommendations include enhancing technical expertise, fostering collaboration, continuous threat monitoring, allocating sufficient budget, developing tailored strategies for phishing attacks, and strengthening public-private collaboration. Limitations include a small sample size and potential biases in participant responses. This research contributes to the understanding of cybersecurity resilience and provides actionable insights for policymakers, practitioners, and researchers in the field.

Keywords Cyber Security Resilience, Critical infrastructure, Cyber Threats

1. Introduction

Cyber resilience spans multiple levels of operation, including organizational, functional, technical, natural, regional, and supernatural. It is the capacity to continuously produce desired results in the face of unfavorable cyber occurrences (Björck et al., 2015). Cyber resilience is applicable to corporations and individual IT systems in addition to nations, with each level presenting unique difficulties, solutions, and potential controls. Cyber resilience, however, needs to be addressed on many levels at once and with a holistic approach in order to be effective. Continuity refers to the ability to continue with operations in the face of disasters, channel outages, or cyberattacks. It entails returning the scene to normal after the event and continuously modifying delivery methods in response to new dangers. Cyber resilience is distinct from normal business resilience in that it is centered on the negative cyber events that impact networked IT systems. The danger landscape is constantly changing due to society's growing reliance on sophisticated cyber systems for everyday tasks. Examples of

these threats include viruses, code alterations, Distributed Denial-of-Service (DDoS) attacks, and data breaches. Cyber dangers constantly affect people, companies, and governments, with serious ramifications for personal safety, financial stability, and national security. Conventional hardening techniques are unworkable due to the inability of traditional risk assessment methodologies to handle the dynamic nature of cyber threats and the complexity of interconnected systems. Thus, building cyber resilience entails anticipating, absorbing, recovering from, and adjusting to negative effects, especially those resulting from cyberattacks. To put it briefly, cyber resilience is the ability of a system to endure and bounce back from unfavorable cyber occurrences. Proactive tactics, flexible systems, and all-encompassing methods are required to lessen the dynamic threat environment and protect vital infrastructure systems.

The aim of this study is to assess the resilience of cyber security measures in regulating critical infrastructure within Zambia. This involves examining the existing strategies employed by IT managers and compliance officers to mitigate cyber threats, identifying the forms and nature of cyber-attacks prevalent in Zambia, and developing a robust framework to enhance cyber resilience against these threats. The study will provide insights into the current state of cyber security, evaluate the preparedness of critical infrastructure

* Corresponding author:

gmweembe@yahoo.com (Grenah Sivwimi)

Received: May 23, 2024; Accepted: Jun. 20, 2024; Published: Jul. 6, 2024

Published online at <http://journal.sapub.org/computer>

against cyber threats, and propose strategic measures to strengthen cyber resilience in Zambia.

2. Statement of the Problem

In an increasingly interconnected digital landscape, safeguarding critical infrastructure against cyber threats has become paramount for national security and economic stability. As cyber-attacks continue to evolve in sophistication and frequency, it is imperative to evaluate the resilience of cyber security measures in regulating critical infrastructure. Furthermore, Zambia, like many other developing countries, is perceived as having insufficient capacity and capability to effectively counter these sophisticated cyber security threats and cyber-attacks, which are increasingly gaining world attention. According to a recent report by Markaday (2022), with Africa's internet penetration the highest in the world, there has been an increase in cybercrime, costing the continent billions in lost GDP (\$4.12 billion in 2021). In Zambia, there is still a gap in cyber security awareness, making more people and organizations vulnerable.

3. Research Objectives

- a. What IT cyber security strategies are used by IT managers and compliance officers to mitigate cyber threats to critical infrastructure?
- b. To identify the forms of cyber-attacks in Zambia.
- c. To develop framework that can be used to curb cyber-attacks.

4. Research Questions

- a. What are the critical infrastructures which might be targeted for cyber-attacks? What are the existing strategies against cyber-attacks preparedness in Zambia?
- b. What is the nature and the forms of cyber-attacks? What are the weapons and sources of?
- c. What are the appropriate frameworks and strategies that can be used to curb cyber-attacks in Zambia?

5. Related Works

Another researcher concludes that his Comparative results show that Bayesian networks were more accurate and much faster than Artificial Neural Networks to train when detecting fraud, but Bayesian networks are slower when applied to new instances. (Maes et al, 2002)

A study by Adedoyin (2018), Predicting Fraud in Mobile Money transfer which was aimed at investigating a pattern recognition model to predict fraud in mobile money transfer transactions in the United Kingdom. The study evaluated the recognition model using the simulation dataset. The findings of this study gave proved that the pattern recognition performed

well in mobile money prediction.

A study by Maruatona (2013) Internet Banking Fraud Detection using Prudent Analysis in Australia. The study was aimed at developing and evaluating a system for use in Internet banking Fraud detection using Prudence Analysis in a Ripple down Rules (RDR) system. This study applied the rule-based system approach combined with Artificial Neural Network (AAN) to security and fraud detection. The findings of this research indicated that a prudent system is a viable alternative in an online banking fraud detection.

The dataset comprised 40 attributes and consisted 1760 transactions 60% of which were legitimate and 40% were fraudulent.

A research by Alanezi (2015) the Perception of online fraud and the impact on the countermeasures for control of online fraud in Saudi Arabian Financial institution. This study addresses the impact of countermeasures in the control and prevention of online fraud in Saudi Arabia. This research aimed to examine online fraud perceptions and the countermeasures designed and used by financial institutions in Saudi Arabia to control and prevent online fraud in its environmental context. This study addressed the impact of countermeasures in the control and prevention of online fraud in Saudi Arabia. The qualitative method approach was chosen to ensure balanced coverage of the subject matter. The findings show two types of regulations: government and organizational rules, with different foci and purposes, which are mostly centered on the monitoring of Internet operations and operational guidelines.

Amrin (2014) examines the Impact of cyber Security on SME's using Cloud Computing & Bring Your Own Device in multiple SME's in Europe. The findings were that IT Security of respondents on SME's is not a decent point. Furthermore, Amrin's findings were that Cloud computing and BYOD was accepted technology among the respondents but the respondents of the SME's were not aware of the vulnerabilities related to BYOD and Cloud computing.

Cyber threats in Southern Africa and Zambia

According to Markanday (2022), in South Africa, businesses that fail to report cyber-attacks in accordance with the law face fines of up to R50, 000. South Africa, the economic hub of the region, has the third highest number of cybercrime victims in the world, costing its economy R2.2 billion a year.

The research by Afriwise also makes a startling observation: although many African countries have enacted cyber security laws, they lack the capacity and infrastructure to enforce these legislations.

Further, there is a dire shortage of critical skills, with far few professionals in the sector, and too few in decision-making positions in the regulatory industry. "Therefore we have people making laws without the expertise needed and, simultaneously, lawyers without the expertise needed to enforce the laws that have been passed".

It looks likely that Zambia isn't any different from other African countries. But the Zambian government is keen on protecting essential services by making sure it "uplifts the

security and resilience of infrastructure on which critical information lies".

"As the threats and risks to Zambia's CII evolve in a post Covid world, so too must the approach for ensuring the ongoing security and resilience of CII and the essential services they support," says the Zambia Information, Communication and Technology Authority (ZICTA) in a concept note explaining the rationale and motivation around the proposed regulations.

ZICTA believes using local cloud service providers "will help grow the Zambia cloud service industry and investments in the ICT sector", and that this will help create jobs and boost opportunities in the space.

Further, ZICTA believes that it will be easier to investigate and resolve cyber-attacks if the data compromised is within Zambia's jurisdiction, an assertion based purely on not understanding cybercrimes in a world where the concept of a global village is real and where we are all connected.

Although ZICTA suggests that governments worldwide are moving in the same direction, there is no evidence of this.

Widespread consultations have been held, and some investors have made submissions pointing out the weaknesses around the approach by the government, and arguing for self-regulating safeguards that businesses apply to counter concerns raised by ZICTA.

6. Methodology

6.1. Methods and Data Collection

The research employed a descriptive research design, utilizing questionnaires as the primary data collection instrument. The study population comprised the Information Technology regulation board of Zambia (ZICTA), Airtel, and MTN, Zanaco, National Airport Corporation, Zambia Police Service, DEC, ICTAZ, UNZA, Mulungushi University, CBU and ZCAS. A sample size of 543 individuals from the above organizations in Zambia was determined using purposive and random sampling techniques. Primary data, gathered through questionnaires distributed among IT professionals specializing in Cybercrime division, was complemented by secondary data sources. The questionnaire facilitated the exploration of participants' awareness, effectiveness of cybersecurity strategies, challenges in implementation, prevalent cyber- attacks, views on cybersecurity frameworks, and collaboration between policymakers and the private sector.

6.2. Analysis and Results

Data analysis was conducted using qualitative approaches, focusing on content analysis to address the research objectives. Descriptive statistics, including maximum, minimum, mean, and variance, were utilized for data presentation. The results revealed a nuanced understanding of cyber resilience across different levels, with respondents demonstrating extensive awareness of current cybersecurity strategies but expressing concerns about their effectiveness. Challenges identified included limited technical expertise, lack of collaboration, rapidly evolving threats, and budgetary constraints. Phishing

attacks emerged as the most prevalent form of cyber-attacks on critical infrastructure in Zambia, influencing stakeholders' views on the importance of cybersecurity policies. The majority of respondents advocated for a comprehensive framework tailored to curb cyber-attacks, emphasizing the need for regular cybersecurity audits and strong collaboration between policymakers and the private sector.

7. Findings

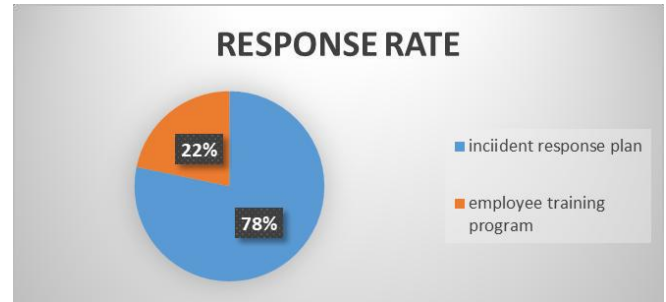


Figure 7.1. Shows the Response Rate

According to the above information out of 543 respondents 361 respondents answered the questionnaire. The above results state that 66.7% of the respondents answered the questionnaire.

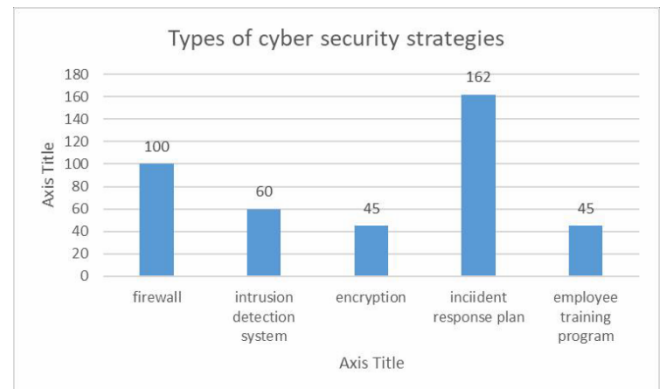


Figure 7.2. Types of cyber security strategies employed

According to the above information, 100 respondents had firewalls as a security strategy, 60 had in Intrusion Detection systems as a security strategy, 45 respondents had encryption as a security strategy, 162 respondents had incident response plan as a security strategy, 45 respondents had employee training programs as a security strategy.

8. Discussion of Research Findings and Analysis

8.1. Discussion

The interpretation of findings underscores the critical need for a comprehensive and adaptive cybersecurity framework to address the identified challenges and enhance the effectiveness of current strategies. The discrepancy between awareness

and perceived effectiveness highlights potential gaps in cybersecurity preparedness. Addressing challenges such as limited expertise and collaboration requires concerted efforts from stakeholders across various sectors. The prevalence of phishing attacks underscores the importance of targeted strategies to combat specific threats within the cybersecurity framework. Strong support for collaboration between policymakers and the private sector reflects a collective understanding of shared responsibility in safeguarding critical infrastructure. Overall, the findings emphasize the dynamic nature of cyber threats and the imperative for proactive, collaborative, and adaptive approaches to cyber resilience in Zambia.

8.2. Conclusions

The research underscores the paramount importance of cyber resilience in safeguarding critical infrastructure against evolving cyber threats. Despite extensive awareness of current cybersecurity strategies, stakeholders' express concerns about their effectiveness in addressing cyber threats. The identified challenges, including limited technical expertise, lack of collaboration, and budget constraints, highlight the multifaceted nature of cybersecurity preparedness. Phishing attacks emerge as a predominant threat, emphasizing the need for targeted strategies within the cybersecurity framework.

The findings emphasize the imperative for a comprehensive and adaptive cybersecurity framework tailored to curb cyber-attacks on critical infrastructure in Zambia. Collaboration between policymakers and the private sector is essential for developing and implementing effective cybersecurity policies. Continuous threat monitoring and regular cybersecurity audits are crucial for staying ahead of evolving threats and mitigating vulnerabilities.

In conclusion, the dynamic nature of cyber threats necessitates proactive, collaborative, and adaptive approaches to cyber resilience. The recommendations outlined in the study, including enhancing technical expertise, fostering collaboration, and developing tailored strategies, provide a roadmap for strengthening cybersecurity preparedness in Zambia. By addressing the identified challenges and implementing the proposed recommendations, stakeholders can enhance the resilience of critical infrastructure and mitigate the impact of cyber threats on national security, economic stability, and social well-being.

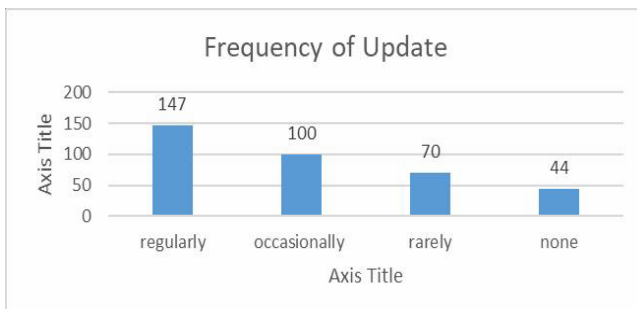


Figure 8.1. frequency of Systems Update

Out of 361 respondents; 147 respondents regularly carried out security updates, 53 respondents occasionally carried out security updates, 70 respondents rarely carried out security updates and 30 respondents did not carry out security updates.

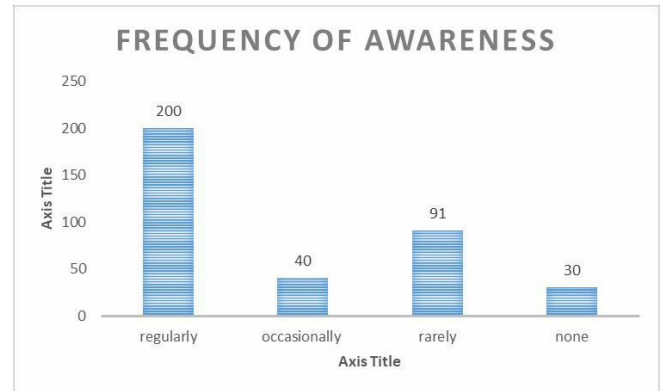


Figure 8.2. Frequency of awareness trainings

Out of 361 respondents; 200 respondents regularly carried out security Awareness, 40 respondents occasionally carried out security Awareness, 91 respondents rarely carried out security Awareness and 30 respondents did not carry out security Awareness.

8.3. Equations

$$n = N * X / (X + N - 1),$$

Where,

$X = Z_{\alpha/2} - *p * (1-p) / MOE^2$, and $Z_{\alpha/2}$ is the critical value of the Normal distribution at $\alpha/2$ (e.g., for a confidence level of 95%, α is 0.05 and the critical value is 1.96), MOE is the margin of error, p is the sample proportion, and N is the population size.

ACKNOWLEDGEMENTS

I would like to appreciate my supervisor, Dr Simon Tembo, who relentlessly, guided me throughout the research project to ensure its completion and that it is completed in acceptable standards. I am immensely grateful to him for his professional guide, encouragement, wisdom and constant reminder to make progress. I would also like to thanks my colleague and classmate, Rodgers, who kept inspiring me to reach my goal.

During this research writing, I interacted with a lot of intellectuals in the ICT sector from many organizations. During data collection, findings and results compilation, I worked with individuals whose input was so vital for this research, like Milimo Munyati from ZAMTEL and Mr Nawa from ZICTA to mention but just a few. I benefited from many other individuals from other organizations whom I visited during data collection who in one way or another contributed to the success of this research.

I would like to dedicate this paper to my children Ephraim, Changu, Kanji and Twalumba. They allowed their quality time with mom to be taken over by academic activities. They

spent several nights and went to bed alone without mom. I was encouraged and motivated to complete this work so I can set a standard of lowest level of education to my children. I thank them sincerely to allow me share the resources for their own education and expenses for my project.

Lastly, I would like to dedicate this paper to my ever supporting husband, Fredrick Muleya. His belief in me that I can always get what I set my mind to do, propelled me to go higher and higher and bring home success. He stood in for me with our kids. He waited on me whilst I studied and cheered on that, I could do it. I owe him atleast, this paper.

REFERENCES

- [1] Adedoyin, A. (2018), Predicting Fraud in Mobile Money transfer.
- [2] Airtel Zambia. (17 December 2019). About Airtel. Retrieved from https://www.airtel.co.zm/home_investor_zm.
- [3] Alashan, S., Joshi, S. & Mikkelen, D. (2019). Financial crime and fraud in the age of cyber security.
- [4] Albert, M. R. (2002). E - buyer beware: why online auction fraud should be regulated. *American Business Law Journal*, 39(4), 575-644.
- [5] Alanezi, F. (2015) the Perception of online fraud and the impact on the countermeasures for control of online fraud in Saudi Arabian Financial institution.
- [6] Amrin, N. (2014). The Impact of Cyber Security on SME's Cloud computing & BYOD.
- [7] Anwar, S., & Loughran, T. A. (2011). Testing a Bayesian Learning Theory of Deterrence among Serious Juvenile Offenders. *Criminology*, 49(3): 667-698.
- [8] Aghatise, J. (2014). Cybercrime definition. Retrieved from https://www.researchgate.net/profile/Joseph_Aghatise/publication/265350281_Cybercrime_definition/links/5409af300cf2822fb73b5a2f/Cybercrime-definition.pdf.
- [9] Aron, J. (2018). Mobile Money and the Economy: A Review of the Evidence.
- [10] Arlitscha, K., & Edelman, A. (2014). Staying safe: Cyber security for people and organizations.
- [11] A Report from United Nations offices on drugs and crime (UNODC). The use of the Internet for terrorist purposes, New York, USA, 2012.
- [12] Atanu, D., Hyejung, K., & Gill, R. (2014). Mobile Money Opportunities for Mobile Operators. In: *Business & Network Consulting, Huawei Technologies White Paper*.
- [13] Bank of Zambia. (2019). Bank of Zambia Journal. Retrieved from www.boz.zm.
- [14] Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland. (2014). "Data mining for credit card fraud: A comparative study," *Decision Support Systems*, vol. 50, 2011.
- [15] Beck T. Cull R. (2013). "Banking in Africa." Policy Research Working Paper 6684, World Bank Washington, DC.
- [16] Bersudskaya, Vera, and Dorieke Kuijpers. 2016. "Agent Network Accelerator Survey: Uganda Country Report 2015." Helix. <http://www.helix-institute.com/data-and-insights/agent-network-accelerator-survey-uganda-country-report-2015>.
- [17] Bank of Zambia (2017) Annual Report, Lusaka, Zambia.
- [18] Brown, S. (2005) "Telecommunication fraud management Retrieved from: http://waveroad.ca/ressources/Whitepaper_SB_Janvier2005.pdf.
- [19] Owen, D. R. J., and Hinton, E., 1980, Finite elements in plasticity-theory and practice, Pineridge Press, Swansea.
- [20] Pise, P. J., 1982, Laterally loaded piles in a two-layer soil system., *J. Geotech. Engrg. Div.*, 108(9), 1177-1181.
- [21] Poulos, H. G., 1971, Behavior of laterally loaded piles-I: Single piles., *J. Soil Mech. and Found. Div.*, 97(5), 711-731.
- [22] Reese, L. C., and Matlock, H., 1956, Non-dimensional solutions for laterally loaded piles with soil modulus assumed proportional to depth., *Proc., 8th Texas Conf. on Soil Mechanics and Foundation Engineering*, Austin, Texas, 1-23.
- [23] Reese, L. C., and Welch, R. C., 1975, Lateral loading of deep foundations in stiff clay., *J. Geotech. Engrg. Div.*, 101(7), 633-649.