Journal of Management Sciences, Innovation, and Technology (JMSIT)

https://journals.cut.ac.zw/index.php/JMSIT

Developing a cyber-security governance framework for Zimbabwe local authorities: Challenges and Solutions

Chundu, Brian [1], Sifile, Obert [1], Masamha, Tavengwa [1]

[1] Chinhoyi University of Technology, Zimbabwe

ABSTRACT

The study investigated challenges faced by Zimbabwe local authorities when developing a cyber-security governance framework. This study employed exploratory research which induced a qualitative study guided by the interpretivist philosophy. The case study surveyed Harare, Bulawayo, Gweru, Masvingo and Mutare local authorities. Semi-structured interviews were used to gather data, and forty respondents were chosen using purposive sampling. The study employed structural coding and thematic analysis as data analysis techniques and the software tool used for coding and data analysis was Maxqda. In addition, document review, social media and literature review were used to triangulate data from interviews to strengthen validity and reliability of the study. The results of the study showed that the presence of politics, economic hardships, lack of adaptability to technological changes, obsolete IT infrastructure, and lack of corporate governance practices are major factors which negatively impact the development of a cyber-security governance framework for Zimbabwe local authorities. As such, the study proposed a model with measures to counter these challenges. The proposed model enhances risk management processes, improve regulatory compliance, increase stakeholder confidence, and improve operation efficiency in Zimbabwe local authorities. However, the major limitation of the study was that, only views from the selected five urban local authorities were obtained out of ninety-two local authorities in Zimbabwe.

Key words: Cyber-security, Governance, Challenges, Framework, Local authorities

Introduction

The study investigated challenges faced by Zimbabwe local authorities when developing cyber-security governance framework. Cyber-security governance refers to technological practices, establishing frameworks and policies which safeguards organisations from cyber-threats (Shaker et al., 2023). In the context of this study, cyber-security governance is the protection of Zimbabwe local authorities' computer application systems, data and network infrastructure from cyber-threats. Developed nations and their organisations had put systems and frameworks in place which govern cyber-security. Correspondingly, the growth in the use of technology and adoption of information technology governance frameworks like the National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technologies (COBIT), Information Technology Infrastructure Library (ITIL), and ISO 38500 has shown chances for the economic growth to people and organisations using cyber-space (International Telecommunication Union (ITU) (2024). These frameworks guide organisations in managing risks, decision making, compliance and accountability. Similarly, Zimbabwe information security is being administered by the Cyber and Data Protection Act, 2021, a framework for data security and cyber-security management (Government of Zimbabwe, 2021).

However, the growing of technologies has caused nations world-wide including Zimbabwe to be exposed to cyber-threats (Zimbabwe National Risk Assessment Report, 2021). Additionally, cyber-threats have a huge impact on the sustainability of businesses and the economy. Globally, popular cyber-attacks lead to identity theft, corporate extortion, and loss of confidential information and customer databases (Africa Cyber-Security Report, 2024). In Zimbabwe, both private and public organisations including local authorities are more exposed to vulnerabilities such as computer related forgery and frauds, data espionage, identity theft, phishing attacks, hacking, and online harassment among others (Bulawayo 24, 2021). Zimbabwe local authorities are failing to mitigate these cyber-threats because they encounter a lot of predicaments when developing a cyber-security governance framework. Thus, the study provided a model with measures to mitigate setbacks which hinder the process of developing a cyber-security governance framework. This paper comprises of the introduction, literature review, methodology, results findings, discussion and the conclusion.

Objectives of the study

a. To identify challenges faced when developing a cyber-security governance framework for Zimbabwe local authorities.
b. To propose a model with solutions to mitigate cyber-security governance framework challenges.

Literature review

Cyber-security governance in Zimbabwe local authorities

The Constitution of the Republic of Zimbabwe provides a system of local government which facilitates social-economic development with a vision of improving infrastructure for urban and rural towns (Government of Zimbabwe, 2013). Zimbabwe local authorities govern the affairs of the local citizens through elected councillors and appointed technocrats (Dube, 2019). Zimbabwe local authorities provides public service delivery to the nation, and this includes water supply and sanitation, waste management, urban and rural development, roads and infrastructure, health services, education services, and community development and social services .The Zimbabwe National Development Strategy 2 (2025 – 2030) framework

empowers local authorities to embrace digitalisation and adopt the key principles of cyber-security governance in order to improve service delivery and attain Zimbabwe Vision 2030.

Like any other government institutions in the world, Zimbabwe local authorities are digitalising to ensure that they provide an effective service delivery under a low-cost operation (Government of Zimbabwe, 2021). In May 2021, Zimbabwe local authorities through the Ministry of Local Government Public Works and National Housing introduced the Local Authorities Digital System (LADS) which comprises of the Enterprise Resource Planning (ERP) System and an Integrated Financial Management Information System. The LADS electronically link local authorities in Zimbabwe for procurement, project management, risk control, compliance, fiscal performance, budgets and expenditures, and financial statements (Ministry of Local Government Public Works and National Housing, 2022). Thus, LADS is being launched to all Zimbabwean local authorities in line with information technology governance programmes.

However, the introduction of digitalisation and the management of cyber-security governance in local authorities come with its challenges, given the economic meltdown of developing countries and political interference (Kabwe et al., 2024). In addition, Kabwe et al. (2024) argue that the issues of lack of skilled personnel and insufficient regulatory frameworks contribute more to the challenges faced by local authorities when they develop their information technology governance frameworks.

Theoretical framework

The study was guided by the Game theory. The Game Theory postulates how organisations and their people (called players) connect to make strategic decisions about business operations and situations (Katz & Butler, 1994). In addition, the Game theory enables the modelling of interaction, resolves conflicts and enables organisations to make tactical choices (Ho et al., 2022). However, the theory is subjective and requires judgement and expertise when implementing. In the context of this paper, the theory provides a strategic direction and governance principles by the local authority boards and all their stakeholders on identifying cyber-security governance challenges and putting strategies to counter the challenges.

Empirical review

The studies conducted by different researchers in developing countries have indicated the development of information technology governance frameworks and the digitalisation of organisations and government institutes. A study conducted by Ramodula and Govender (2020) highlighted that scarcity of resources, corruption, and mismanagement were challenges which obstructed the development of local governance systems in South Africa. To mitigate these challenges, the scholar recommended that South African Municipalities were to adopt corporate governance practices of transparency, accountability and citizenship participation. Correspondingly, a study conducted by Kabwe et al (2024) concluded that lack of information communication technology infrastructure affected negatively the process of digitalisation in Zambian local authorities. Furthermore, a comprehensive study conducted by Mutoya (2024) pointed out that devolution and the alignment of Zimbabwean laws with the Constitution of Zimbabwe improves service delivery of Zimbabwe local authorities. However, these studies indicate that there was a gap concerning challenges faced by Zimbabwe local authorities when developing a cyber-security governance framework. Thus, the study wanted to fill the gap by investigating these challenges and coming up with a model to counter them.

Conceptual framework

The conceptual framework of this study reflects on the need to identify challenges faced by Zimbabwe local authorities when developing and cyber-security governance framework and coming up with strategies to mitigate the challenges. Figure 1 summarises the conceptual framework of the study.

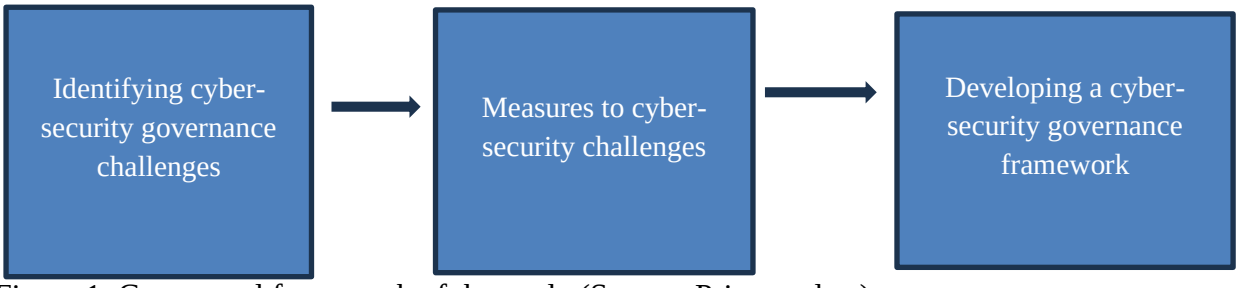

Figure 1: Conceptual framework of the study (Source, Primary data)

Methodology

The study adopted the interpretivism which enabled the researchers to improve their deep perceptions into cultural meanings that form individual behaviour. In addition, an exploratory research design which motivated the use of qualitative data was employed. The exploratory research design made the researchers to explore the study from different dimensions (Saunders, 2024). The study population was chosen from the five urban local authorities namely Cities of Harare, Bulawayo, Gweru, Mutare and Masvingo. The local authorities had a population of 17292 employees (Ministry of Local Government Public Works and National Housing, 2023). These local authorities had advanced information technology infrastructure as compared to Municipalities, Town Councils and Rural District Councils and, they shared same organisational structures (Ministry of Local Government Public Works and National Housing, 2023). Thereafter, a sample of forty respondents that is eight from each local authority was selected through purposive sampling technique. Amongst the eight respondents, four came from top management and the other four were from information technology department. These respondents had knowledge of formulating and implementing information technology governance frameworks.

Data was collected through semi-structured interviews, document analysis and social media platforms. A pilot study was conducted first to improve the semi-structured interview guide. The semi-structured interviews took an average of thirty minutes to an hour and they enabled the interviewer to get detailed responses and probe responses whenever he needed clarity. In addition, the interviewees were coded in alphabetical order from A to Z and A1 to M1 to remain unidentified and, local authorities were given codes namely X1, X2, X3, X4 and X5. With the interviewee's consent, the interviews were recorded using a cell phone. Editing of the transcribed text was done through listening and grammatical errors were corrected. Furthermore, data analysis software Maxqda was used to analyse interview transcripts, and secondary documents gathered on cyber-security governance. Also, it was used to explore themes. Social media platforms were used to analyse the current state and challenges of Zimbabwe local authorities and the anticipated outcomes and preferred standards by the general population. Thereafter, data was triangulated. As noted by Miles and Huberman (1994), triangulation of data improves trustworthiness, integrity and dependability of research findings.

Ethical consideration

The Chairperson of Chinhoyi University of Technology Research and Innovation Committee granted authority to conduct the research through a clearance letter with reference number GRSD 17 SEBS 30/2023.The research clearance letter was submitted to the responsible authorities of the five selected local authorities under study who granted permission to conduct the study via letters and emails.

Research findings and data analysis

Challenges faced by Zimbabwe local authorities when developing a cyber-security governance framework

Corporate governance issues

The interviewee's response underscored a collection of corporate governance issues that impeded the development of a strong cyber-security governance framework for Zimbabwe local authorities. These included corruption, lack of accountability, lack of independence of the local authority boards, transparency, non-disclosure of conflict of interests and favouritism/nepotism. Furthermore, the interviewees highlighted that lack of independence among the board of directors lead to prejudiced decision-making which obstructed the formulation of robust cyber security governance framework. This suggests that corporate governance issues weakened efforts to formulate an effective cyber-security governance framework. Interviewee A, a top manager at from local authority X1 opined that:

> *The challenges faced by Zimbabwe local authorities in developing a cyber-security governance framework are mostly centred on corporate governance issues. These include bribery, dishonesty and lack of accountability*

Lack of Expertise

The interviewees underscored that the lack of personnel with cyber-security governance understanding posed as a significant challenge in the development of a cyber-security governance framework. Zimbabwe local authorities lacked personnel with knowledge and skills required to effectively develop and implement a cyber-security governance framework. Interviewee R, an IT expert from local authority X3 opined that:

> *There is lack of ICT expertise in Zimbabwe local authorities. For example, Zimbabwe local authorities started recruiting ICT managers around 2019 or 2020. All along, ICT administrators who were under the Finance department oversaw ICT in Zimbabwe local authorities.*

In addition, interviewee D, an IT expert from local authority X1 also opined that:

> *Having leaders in Zimbabwe local authorities without a background of ICT is creating more problems because they lack knowledge on how to advocate for an ICT governance framework.*

Economic hardships

The interviewees argued that the absence of enough resources in Zimbabwe local authorities hindered Zimbabwe local authorities the capabilities to capitalise in a cyber-security ecosystem. Additionally, the interviewees noted that economic hardships, including a volatile economy and hyperinflation, pose serious problems to developing a cyber-security governance framework for Zimbabwe local authorities. Furthermore, the interviewees underscored that

inadequate funding for IT projects also posed as a significant challenge. Interviewee A1, a manager from local authority X1 stated that:

> *The economic factors affect the distribution of resources, exchange rates, inflation rates and interest rates.*

Political Influence

The interviewee's mentioned that Zimbabwe local authorities were affected by politics which had an impact on their decision-making processes. According to the interviewees, politicians had an influence towards decisions made by Zimbabwe local authorities, formulation of government policies, and legislations. In addition, the interviewees argued that most Councillors who sit in local authority boards had a limited understanding of cyber-security governance. Furthermore, the interviewees highlighted that the political differences between elected members of parliament, administrators, and technocrats had a negative impact on cyber-security policy formulation. Interviewee O1 a manager at local authority X5 said that:

> *The political influence in Zimbabwe delays the formulation of effective cyber-security governance policies.*

Technological Changes.

The interviewees indicated that a rapid change in technology was another challenge which was being faced by Zimbabwe local authorities when developing a cyber-security governance framework. The interviewees also noted that the quick technological advancements required a perpetual modification and investment, which was difficult to withstand given the economic hardships in Zimbabwe and lack of expertise. The interviewees added that the lack of expertise was caused by low salaries and benefits which made it difficult for Zimbabwe local authorities to attract and retain qualified personnel in the field of cyber-security and IT governance. Interviewee Y, an IT expert at local authority X3 opined that:

We have obsolete IT infrastructure in Zimbabwe local authorities. There are no qualified personnel to administer IT due poor remuneration by Zimbabwe local authorities.

Lack of training and cyber-security awareness

The interviewees highlighted that there was lack of cyber-security awareness and training among employees in Zimbabwe local authorities and their stakeholders. Additionally, they mentioned that the general lack of cyber-security understanding and awareness by stakeholders such as law enforcement agencies, the judiciary, and the responsible Ministry of Local Government Public Works and National Housing as well as the society was a challenge in the development of a cyber-security governance framework for Zimbabwe local authorities. Interviewee I, an IT employee at local authority X2 opined that:

> *Zimbabwe is still at its early stage in fighting cyber-criminals. The citizens are not even aware on how to tackle cyber-security related issues. There is lack of cyber-security training among the citizens and the council officials.*

Role of Zimbabwean government in developing a cyber-security governance framework for Zimbabwe local authorities

Enactment of legislation and policy formulation

The interviewee's highlighted that the Zimbabwean central government contributes to the development of a cyber-security governance framework through the sanctioning of a helpful legislation and providing a policy framework for local authorities to follow in their cyber-security mitigation efforts. This underscores the significance of government participation in founding regulatory and compliance systems to address cyber-security challenges and secure information and critical infrastructure. Furthermore, the interviewee's argued that the central government owns the police and the courts, which are important in combating cyber-threats. This underlines the government's role in supporting law enforcement agents and the judicial in addressing cyber-security challenges. Thus, it is the government's obligation to address socio-political, economic, and cultural matters that may weaken cyber-security efforts. Interviewee F a manager at local authority X1 opined that:

> *To address cyber-security challenges, the government should enact legislation and formulate a cyber-policy which governs the day-to-day operations of Zimbabwe local authorities. This policy can be used as a benchmark by both the public and private organisations when formulating their IT governance frameworks. Legislation can be used to deter cyber-criminals from committing cyber-crimes.*

Emerging themes

The study employed structural coding and thematic analysis as data analysis techniques. According to Miles and Huberman (1994) structural coding is the use of question-based codes which act as a labelling and indexing device, allowing researchers to quickly access data likely to be relevant to a particular analysis from a large data set. In addition, Saldana (2021) define thematic analysis as a methodical process of classifying, examining, and reporting themes within the data. The process of structural coding and thematic analysis enabled the researchers to identify the most recurring patterns which emerged from the interviews. Two major themes emerged from the interviews were identified and summarised as follows: Cyber-security challenges and role of the government.

Cyber-security challenges

> *The major challenge is that there is lack of ICT expertise in Zimbabwe local authorities' structures (Interviewee C).*
>
> *Having members without a background of ICT in top management or board creates a lot of problems because they lack the knowhow on how to advocate for an ICT framework (Interviewee Z).*
>
> *The challenges include political influence, economic constraints, social issues, technological changes, legal framework, and environmental factors. They all affect the development of a cyber-security governance framework. (Interviewee W).*
>
> *The key challenges include funding, staffing issues, and remuneration concerns which collectively hinder the development of effective cyber security governance frameworks within Zimbabwe local authorities (Interviewee E).*
>
> *Resource constraints due economic hardship and lack of leadership support contribute more to challenges faced when developing a cyber-security governance framework (Interviewee S).*
> *There is no transparency and accountability in the way in which Zimbabwe local authorities are managed (Interviewee T)*

The focus is on buying top of the range vehicles and the payment of hefty salaries to top management rather than putting effort in building cyber-resilience institutions (Interviewee Q).

The major challenge is that corruption is rampant in Zimbabwe local authorities from the grassroots to top management (Interviewee A).

Role of the government

Government being the governing board set guidelines for its departments, and they can borrow these from developed countries (Interviewee B).

There is need for a blueprint, or a cyber-security governance framework at national level which can be used for benchmarking. (Interviewee N)

The significant role which the central government play in developing a cyber-security governance framework is on the enactment of laws and legislations in fighting cyber criminals (Interviewee D1).

The government also ensures compliance of all the enacted legislations through monitoring and evaluation. (Interviewee E1)

Discussion of findings

The major objective of the study sought to elicit views on challenges faced by Zimbabwe local authorities when developing a cyber-security governance framework. Overall, the respondents' response underscores key challenges which include funding constraints, staffing issues, remuneration concerns, economic challenges, political interferences, lack of innovation, and corporate governance shortcomings, which collectively disrupt the development of an effective cyber security governance framework for Zimbabwe local authorities. These results concur with a study conducted by Atem (2025) and Thornhill (2014) who provided a complete analysis on IT governance challenges in local authorities emphasizing resource constraints, corruption, politics, lack of regulatory frameworks and enforcement as key areas of concern. In addition, Ncamphalala and Vyas-Doorgapersad (2022) argue that challenges related mostly to leadership affected the process of digitalisation in local authorities. Correspondingly, Mironga and Mironga (2022) points out that the lack of independent board members in local authorities' boards indicates the absence of checks and balance on the balance of power. However, the result of the study contradicts with Dube (2019) whose findings pointed to centralisation of state powers as the main bottleneck at Zimbabwe local authorities that pose challenges for technological growth, and sustainability.

The results of the study also put an emphasis on the central government's position in determining cultural norms, endorsing sound policies and regulations, fighting corruption and cyber- crimes, and offering law enforcement and judicial support. Similarly, a study conducted by (Mutoya, 2024) points out that the type of political system and government in place significantly affect cultural values and beliefs, and corporate governance practices of organisations. A study conducted by Sibanda and von Solms (2019) underscores the importance of a strategic approach by the government for an effective and viable implementation of cyber-security governance framework for local authorities. This suggests that a secure and effective government safeguards a comprehensive cyber-security governance system for Zimbabwe local authorities.

Recommendations

The study contributed to the body of knowledge by proposing a model as shown in Figure 2 with measures to counter challenges faced by Zimbabwe local authorities when developing a cyber-security governance framework. The model enhances effective operations, improved risk management process and ensures regulatory compliance for Zimbabwe local authorities. Furthermore, the output of the study can be used as a benchmark by government departments and the private sector in developing countries when formulating and implementing their cyber-security governance policy.

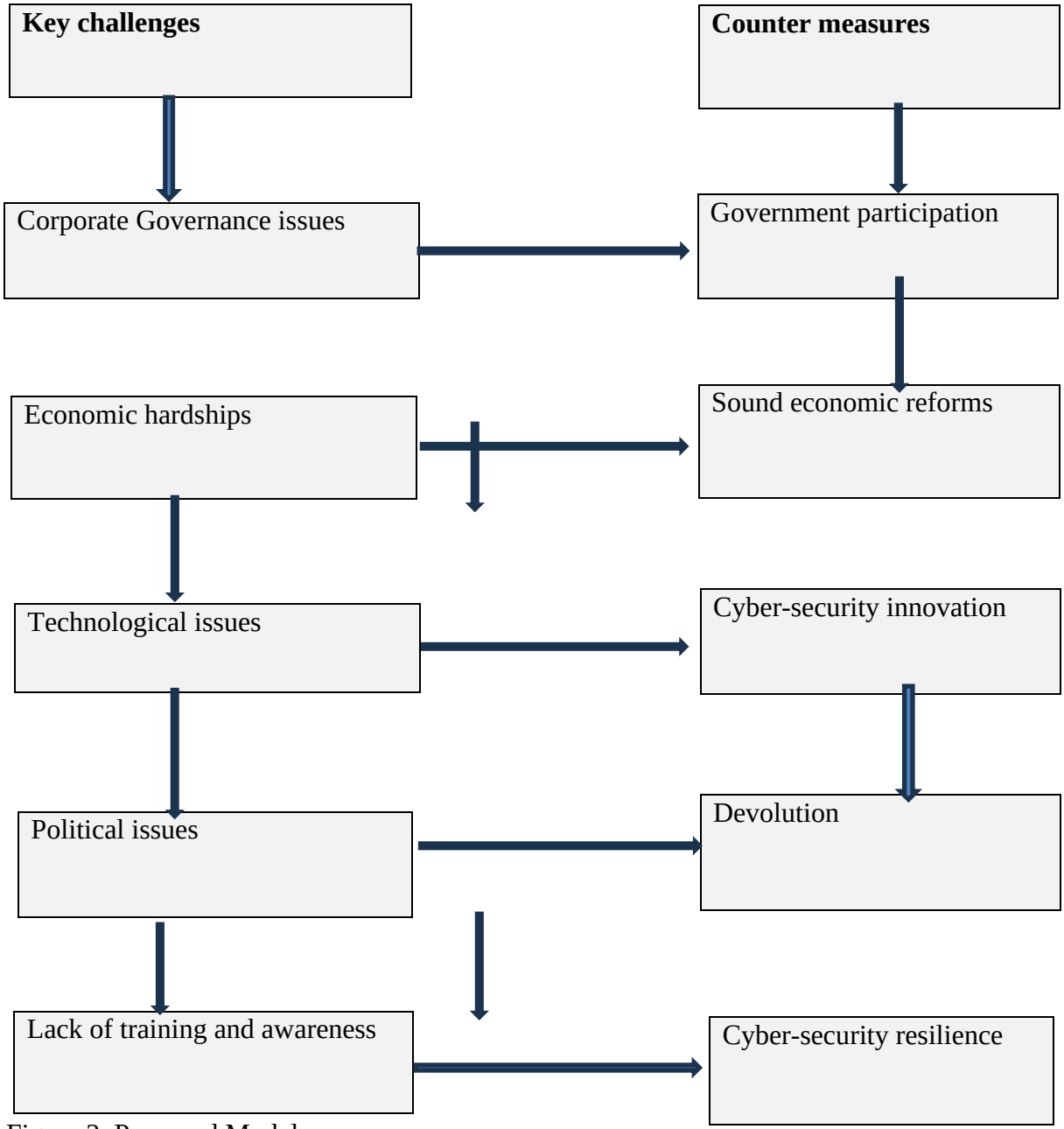

Figure 2. Proposed Model.

Government participation and economic reforms

The government of Zimbabwe should be involved in the development of cyber-security governance framework for Zimbabwe local authorities through provision of leadership, policy

formulation, legislation and compliance. This includes introducing a model for economic growth and social harmony, while also guaranteeing fairness and justice. According to Chundu et al. (2025), the government promote good governance by recruiting competent personnel and putting deterrence measures which punish those who contravenes cyber laws, statutes and corporate governance principles.

Cyber-resilience

Zimbabwe local authorities should have the ability to foresee, survive, and moderate cyber-incidents and threats. This involves the incorporation of cyber-security culture from the grassroots up to leadership level. According to Gcaza (2017), cyber security culture refers to the norms and values, and familiarities of the staff of an organisation with respect to cyber security. Cyber-security culture can be incorporated through training of employees on cyber-security related issues and conducting awareness campaigns. Thus, Zimbabwe local authorities must incorporate a proactive approach to manage cyber-security risk and secure information.

Cyber-security Innovation

Zimbabwe local authorities should develop an innovative mind set which genuinely comprehends the values of cyber-security governance. Savas and Karata (2022) defines cyber-security innovation as a process of addressing cyber-threats through creating new technologies and systems like artificial intelligence, machine learning and cloud-based solutions to prevent and detect all forms of cyber-attacks. Thus, innovation enhances Zimbabwe local authorities to improve in decision making, foster a culture of agility within cyber-security governance framework, manage cyber-risk in a better way, and reduce costs.

Devolution

Chakunda and Matega (2024) define devolution as the decentralisation of power from the national government to regions, provinces, districts and local authorities. Nyikadzino and Vyas-Doorgapersad (2022) argues that the devolution of governmental powers warrants the acknowledgements of local governments as lawful and independent entities and supports their ability to problem-solving. In the context of Zimbabwe local authorities, devolution enables community involvement when formulating cyber-security governance policies, and incorporates different stakeholders, ensures independence of the local authority boards thereby improving the best practices of good corporate governance.

Conclusion

Considering the above outcomes, the study concluded that poor corporate governance, lack of expertise, economic hardships, political influence, technological changes, centralisation of decision making, and lack of training and awareness on cyber-security issues were the major challenges which affected the development of a cyber-security governance framework for Zimbabwe local authorities. Furthermore, the study revealed that the government has a responsibility to formulate policies which governs the development of a cyber-security governance framework. Lastly, a model with measures to counter cyber-security governance challenges was proposed. These measures include government participation, sound economic reforms, cyber-resilience, cyber-security innovation, and devolution.

Limitations of the study

The authors acknowledge that the outcomes of this research were based on the perspectives of participants from the only five selected urban local authorities in Zimbabwe out of ninety-two local authorities. Opinions from rural district councils were not gathered hence, the generalizability of the study is narrow. However, the study outcomes could be customized and

lowered to fit the requirements of cyber-security governance for Municipalities, Town Councils and Rural District Councils.

Areas of future research

Future research should focus on a quantitative study focusing on both urban and rural authorities developing a model with measures to counter challenges faced when developing a cyber-security governance framework.

References

Africa Cyber-Security Report (2024). *Interpol African Cyber-threat Assessment Report 2024*. Available on https://www.linkedin.com/posts/interpolout-now-the-2024-african-cyberthreat-assessment-activity-7192188390212083712-Tnsi/

Atem, E. (2025) Assessing the Gaps in Cyber-security Resilience in Cameroon: Challenges and Opportunities for Strengthening National Cyber-security Frameworks. *Journal of Computer and Communications*, 13, 191-206.

Bulawayo 24. (April 18, 2021): *Italy offers cyber security training in Zimbabwe*. Retrieved from https://bulawayo24.com/index-id-news-sc-local-byo-202538.html

Chakunda, V., & Matenga, G. (2024). Interrogating the Feasibility and Efficacy of Devolved Regional Governments in Zimbabwe Regional and Federal Studies. Available on https://www.researchgate.net/publication/383966672_Interrogating_the_feasibility_and_efficacy_of_devolved_regional_governments_in_Zimbabwe.

Chundu, B., Masamha, T. & Sifile, O. (2025). Cyber-security Governance Framework Pillars for Zimbabwe local authorities. *Cogent Social Science. Journal of Law, Criminology and Criminal Justice*, 11(1),1-11.

Dube, C. (2019). *Main bottlenecks at the local authority level that could pose challenges for growth and sustainability.* Zimbabwe Economic Policy Analysis and Research Unit, Harare.

Gcaza, N., & Von Solms, R. (2017). A strategy for a cyber-security culture: A South African perspective. *The Electronic Journal of Information Systems in Developing Countries*, 80(1), 1–17.

Government of Zimbabwe (2013). Constitution of Zimbabwe Amendment (No 20). Available onhttps://www.veritaszim.net/sites/veritas_d/files/Constitution%20of%20Zimbabwe%20Amendment%20%28No.%2020%29.pdf

Government of Zimbabwe. (2021). (2025-2030). *National Development Strategy (NDS-2)*- Retrieved from https://zimembassydc.org/wp-content/uploads/2023/12/Zimbabwe-Vision-2030.pdf

Ho, E., Rajagopalan, A., Skvortsov, A., Arulampalam, S., Piraveenan, M. (2022). Game Theory in Defence Applications: A Review. *Sensors*, (22) 1032

International Telecommunication Union (2024).Global Cyber-Security Index 2024. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

Kabwe, K., Zhou, C., Jardim, L. & Surguladze, E. (2024). Empowering Societal Digital Transformation at the Local Level. A Case Study of Pemba Town Council. *Digital Policy Studies (DPS).* 3(1)

Katz & Butler (1994). "Game Commander"-Applying an Architecture of Game Theory and Tree Lookahead to the Command-and-Control Process, *Proceedings of the Fifth Annual Conference on AI, Simulation, and Planning (AIS94),* Florida, 1994.

Miles, M. B., & Huberman A. M. (1994). *Qualitative data analysis: An expanded source book* (2nd ed.). Thousand Oaks, CA: Sage Publications.

Ministry of Local Government, Public Works and National Housing (2022). Acts. Retrieved from https://www.mlg.gov.zw/

Ministry of Local Government, Public Works and National Housing (2023). Acts. Retrieved from https://www.mlg.gov.zw/

Mironga, A. & Mironga, M. (2022). A Critical Analysis of the Performance of Local Governments in Zimbabwe under the COVID-19 Pandemic. *Advanced Journal of Social Science10* (1), pp: 75-87.

Mutoya, L. (2024). Management of Local Authorities in Zimbabwe. What needs to be done to improve the Situation? *Africa University of Zimbabwe College of Peace, Leadership and Governance.*

Ncamphalala, M., & Vyas-Doorgapersad, S. (2022). The Role of Information and Communication Technology (ICT) on the Transformation of Municipalities into Smart Cities for Improved Service Delivery. *International Journal of Research in Business and Social Science (2147- 4478)*, *11*(2), 318–328.

Nyikadzino, T. & Vyas-Doorgapersad,S., (2022). 'Zimbabwe's transition to a devolved system of government: Critical factors for success', *Africa's Public Service Delivery and Performance Review* 10(1), a604.

Ramodula1, T., M., & K K Govender, K., K. (2020). Review of the Evolution of the Local Government System In South Africa: Towards Developmental Local Government. *Journal of Public Value and Administrative Insight:*.3(3), p 50-65

Saldana, J. (2021). *The Coding Manual for Qualitative Researchers* (4th ed.). London: SAGE Publications.

Savas, S., & Karata, S. (2022). Cyber governance studies in ensuring cyber-security: An overview of cyber-security governance. *Int. Cyber-security. Law Rev*, *3*, 7–34.

Saunders, M., Lewis, P., & Thornhill, A. (2024). *Research methods for business students (9th ed.)*. Harlow, England: Pearson Education

Shaker, A. S., Al-Shiblawi, G. A. K., Union, A. H., Hameed, K. S. (2023) The Role of Information Technology Governance on Enhancing Cyber-security and its Reflection on Investor Confidence. *Intern. Journal of Profess. Bus. Review 8*(6), 01-23

Sibanda, M., & von Solms. (2019). Devising a strategy for IT governance implementation in municipalities. *The Electronic Journal of Information Systems in Developing Countries*. 85(2), p 1-32

Zimbabwe National Risk Assessment Report (2021). National Payment Systems. Risk Based Guideline on Cyber-Security. Available on https://www.rbz.co.zw/documents/nps/2021/NPS-CYBER-SECURITY-FRAMEWORK-20210427.pdf