CYBERTHREATS AND THEIR IMPACT ON FINANCIAL INTEGRITY: EVALUATING THE EFFECTIVENESS OF LOCAL AUTHORITIES' CYBERSECURITY POLICIES IN PREVENTING AND DETECTING FRAUD

Newman Wadesango [*], Edwin Maveneka [**]

[*] *Corresponding author*, University of Limpopo, Polokwane, South Africa
Contact details: University of Limpopo, 0727 Polokwane, South Africa
[**] Midlands State University, Gweru, Zimbabwe

OPEN ACCESS

How to cite this paper: Wadesango, N., & Maveneka, E. (2025). Cyberthreats and their impact on financial integrity: Evaluating the effectiveness of local authorities' cybersecurity policies in preventing and detecting fraud. *Corporate Law & Governance Review, 7*(2), 32–40.
https://doi.org/10.22495/clgrv7i2p3

ISSN Online: 2664-1542
ISSN Print: 2707-1111

Received: 27.05.2024
Revised: 22.11.2024; 28.01.2025; 18.03.2025
Accepted: 27.03.2025

JEL Classification: C23, D73, G38
DOI: 10.22495/clgrv7i2p3

Abstract

In today's digitally driven public sector, the rapid adoption of technology has improved service delivery but also created a fertile ground for cyberattacks, particularly because many public institutions lack effective cybersecurity policies (Choi, 2021). Cybercrimes such as hacking, phishing, and malware infections pose significant risks, often leading to fraud and accounting scandals that undermine public trust. This research examines the cyberthreats faced by local authorities in Masvingo Province and evaluates the effectiveness of their cybersecurity policies in preventing and detecting these crimes. A quantitative approach was adopted, utilizing questionnaires administered to 80 participants, with data analyzed using SPSS version 23. Findings reveal that local authorities are notably exposed to a range of cyberthreats, with the absence of comprehensive cybersecurity policies and inadequate training being prevalent issues. This study underscores the urgency for the government to develop and implement robust cybersecurity policies for local authorities, with the auditor general tasked to regularly audit their effectiveness.

Keywords: Cyberthreats, Cybercrimes, Local Authorities, Cybersecurity Policies, Fraud, Accounting Scandals, Security Regulation

Authors' individual contribution: Conceptualization — N.W. and E.M.; Methodology — N.W. and E.M.; Software — N.W. and E.M.; Validation — N.W. and E.M.; Formal Analysis — N.W. and E.M.; Investigation — N.W. and E.M.; Resources — N.W. and E.M.; Data Curation — N.W. and E.M.; Writing — Original Draft — N.W. and E.M.; Writing — Review & Editing N.W. and E.M.; Visualization — N.W. and E.M.; Supervision — N.W. and E.M.; Project Administration — N.W. and E.M.; Funding Acquisition — N.W. and E.M.

Declaration of conflicting interests: The Authors declare that there is no conflict of interest.

Acknowledgements: The Authors acknowledge Midlands State University for ethical clearance.

1. INTRODUCTION

According to The Office of the Auditor-General of Zimbabwe (2020), Zimbabwe is home to 92 local authorities, which include 28 urban councils, 4 local boards, and 60 rural district councils. The primary mandate of these local authorities encompasses the provision of essential services, including roads, planning, housing, economic and community development, recreational facilities, and other

amenities (The Office of the Auditor-General of Zimbabwe, 2020). However, as the digital landscape evolves, so too does the potential for cyber threats that can undermine the operational integrity and financial stability of these organizations. Reserve Bank of Zimbabwe (RBZ, 2020) define cyberthreats as any probable hostile attempts aimed at interfering with or causing harm to computer systems. Cybercriminals often target government institutions, including local authorities, recognizing that these entities typically implement weak protective measures against cyberattacks. The motivations behind such cybercriminal activity range from financial gain to the demonstration of power and competition among peers (RBZ, 2020).

Zimbabwe's National Risk Assessment indicates that cybercrime significantly contributes to an estimated annual revenue loss of US$1.8 billion stemming from various illicit activities, drawing attention to the growing need for effective cybersecurity measures (RBZ, 2020). Defined by RBZ (2020) as intentional unlawful activities directed toward individuals, organizations, or governments to inflict harm, cybercrime manifests in numerous forms, including fraudulent transactions, phishing attempts, unauthorized system intrusions, and identity theft. As highlighted in the RBZ (2020), the threat of cybercrime is escalating globally, impacting both public and private sectors. The proliferation of the internet in business transactions has exacerbated the risk, with estimated revenues from cybercrime accounting for approximately 3% to 5% of the global gross domestic product (GDP).

Further validating the urgency of this issue, RBZ (2020) postulate that unauthorized intrusions into governmental systems, including local authorities, have made vulnerabilities in the public and private information technology realms increasingly evident. Wadesango (2024) emphasizes that many individuals in Zimbabwe have encountered phishing attempts, spam emails, and fraudulent websites aimed at defrauding both the private and public sectors, including local authorities. Given the data-driven environment in which local authorities operate, the rising volume and complexity of data introduce higher risks of loss, theft, or misuse through malicious interference or mismanagement. Such incidents threaten individual privacy and security and can result in critical disruptions to essential services.

As reported by the Zimbabwe Republic Police, various significant cyber threats pose considerable risks to individuals and organizations in Zimbabwe, including phishing, credit card fraud, identity theft, hacking, and unauthorized access. Phishing involves the deceptive acquisition of sensitive information via fraudulent emails, while credit card fraud entails the replication and misuse of cards for fraudulent transactions. Identity theft consists of the unauthorized use of an individual's personal information for malicious purposes, and hacking refers to unauthorized access and manipulation of digital systems. The prevalence of these cyberthreats endangers the security of both individuals and businesses, necessitating urgent attention and prevention measures to mitigate their impacts. Recent notable cybercrime cases in Zimbabwe, like the hacking of the Zimdef bank account resulting in a loss of ZWD 120 million and breaches involving the Judiciary Service Commission and the Zimbabwe Electoral Commission's voter roll, further illustrate the escalating trend of cyber fraud targeting local authorities ("Zimdef suffers a $120 million loss as a result of bank account hacking", 2023; "Cyber terrorists target ZEC", 2022).

This study seeks to explore the effectiveness of local authorities' cybersecurity policies in preventing and detecting fraud, with an emphasis on identifying gaps in the literature regarding the implementation of cybersecurity measures within Zimbabwe's local governance structure. The primary research questions guiding this investigation include:

RQ1: How do current cybersecurity policies of local authorities align with established best practices?

RQ2: What are the prevalent shortcomings that expose these organizations to cyberthreats?

By employing a mixed-methods approach, this study will gather qualitative and quantitative data through surveys, interviews, and case studies to unveil the vulnerabilities in existing cybersecurity frameworks. The findings aim to contribute to a better understanding of cybersecurity challenges faced by local authorities and provide actionable recommendations to enhance their defenses against escalating cyberthreats.

The rest of this paper is structured as follows. Section 2 reviews the relevant literature concerning cybersecurity threats and local governance. Section 3 details the methodology employed for empirical research. Section 4 provides a presentation of the results, along with analysis. Section 5 discusses the main findings. Section 6 concludes the paper.

2. LITERATURE REVIEW

2.1. Theoretical framework

One of the well-known theoretical explanations of cybercrime is the routine activity theory, which was introduced by Cohen and Felson (1979). This criminological theory suggests that certain conditions must be simultaneously present for a crime to occur.

1) A suitable target is present: in this context, a suitable target pertains to an individual, object, or location.

2) There is a lack of capable guardians to prevent the occurrence of crime: the capable or suitable guardians are deterrents such as methods of enhancing security and surveillance, including police patrols, security guards, neighborhood watch groups, door staff, observant employees, friends, and closed-circuit television (CCTV) systems.

3) There is the presence of a motivated offender: this assumption suggests that the existence of a victim is reliant upon the deliberate actions of another person.

The theory suggests that three conditions that enable the commission of a crime must occur simultaneously and in the same location. Cohen and Felson (1979) argued that the routine activity theory certainly applies to cybercrimes irrespective of the classification. They further argued that a crime occurs when there is an opportunity for the crime to be committed. For cybercrime to be successfully committed, the opportunity for crime is multiplied by the simple fact that the criminal is no longer location-bound.

Theoretically driven thoughts, such as those noted above, provide the initial basis for evaluating the suitability or relevance of the routine activity theory technology. However, such investigations

cannot conclusively validate or challenge the theory's ability to provide a satisfactory explanation to cybercrime, which necessitates the empirical examination and evaluation of the theory.

According to routine activity theory, the absence of a guardian to prevent crimes from occurring makes an organization vulnerable to crimes. Cybersecurity policy is one of the effective tools to prevent cybercrimes from occurring.

2.2. Cyberthreats faced by local authorities

According to Karpiuk (2021), cyberattacks in the public sector, including local authorities, can be classified into three categories, namely distributed denial-of-service attack, ransomware, and massive data breaches.

1) Distributed denial-of-service (DDoS): DDoS attacks are carried out through extensive networks of interconnected computers, operating without the knowledge of their owners, to inundate websites and other networks with an overwhelming number of connection requests. These attacks aim to surpass the capacity of the targeted systems, causing them to become unable to function properly.

2) Ransomware: Ransomware is a destructive type of virus that infiltrates network systems, often through unverified emails or software downloads, and disrupts or completely disables certain network functions (Marzuki & Ali, 2024). An example of such an attack is the WannaCry ransomware attack on the National Health Service (NHS) systems.

3) Massive data breaches: Data breaches can occur in two ways: maliciously, when cybercriminals breach the security of network systems to gain access to sensitive information, or accidentally, when information is unintentionally leaked, lost, or mistakenly made public. An example of accidental data breach is when information is inadvertently disclosed or misplaced (Li, 2021; Deda et al., 2024). According to Li (2021), local government and agencies face cybercrimes at an alarming rate. Li (2021) postulates that local authorities are often not encrypted and insecure, with no improvements made to defenses at all. Li (2021) cited that in 2019 incident, cybercriminals took over nearly all of Baltimore city's information technology infrastructure and demanded a ransom of 13 bitcoin (about US$76000) to release the city's systems and data. Hubbard (2019) points out that the top three barriers to successfully guard against cybercrimes in local authorities are incapacity to pay salaries to cybersecurity employees, insufficient number of cybersecurity staff, and lack of funds for cyber mitigation training. Local authorities in the USA faced various types of cyberattack that include denial of services, ransomware, malware infection, and phishing (Ifere et al., 2023).

2.3. Major cause of cybercrime in the South African public sector

2.3.1. Inadequate investment in cybersecurity

Due to the developing nature of South Africa's economy, investing in cybersecurity practitioners may not always be feasible. However, this increases the country's vulnerability to cyberattacks. The analysis conducted has confirmed that the public sector, including local authorities, is a prime target for cyber-attacks. Therefore, there is a pressing need to prioritize investment in cybersecurity within this sector.

2.3.2. Slow development of cybercrime legislation

In the past, South Africa has been slow in implementing legislation related to cybercrime. However, in 2021, significant progress was made with the full implementation of the Protection of Personal Information Act (PoPIA) and the signing of the Cybercrimes Bill into law. These developments are highly significant, particularly considering the substantial rise in cyberattacks leading to data breaches in recent years.

2.3.3. Lack of awareness of cyberthreats

With the growing adoption of technological solutions, an increasing number of South African citizens are being exposed to cyber threats, as evidenced by the rise in cyberattack incidents over the past decade (Rozah & Pujiyono, 2022).

This surge in cyber incidents, particularly those resulting in unintentional data exposure or compromised websites, highlights the lack of experience and technical awareness among South Africans when operating in the cyber realm. This lack of awareness makes South Africans more vulnerable targets for cyber attackers.

2.3.4. Increasing use of information technology

The increasing reliance of South Africans on information technology has led to an expanded cyberthreat landscape. Findings from the analysis conducted indicated that information technology systems in the banking sector and public sector, including local authorities, have been vulnerable to security vulnerabilities on multiple occasions. These technologies, applications, and infrastructure present a substantial risk, particularly when used improperly (Hubbard, 2019).

2.3.5. Cyber attackers taking notice

Hubbard (2019) highlighted that the extensive vulnerability of South Africa's cyberthreat landscape is likely to attract the interest of more sophisticated cyberattackers. While the public sector, including local authorities, has been the primary target of previous cyberattacks, attackers are now expanding their focus to other sectors such as construction, manufacturing, and healthcare. As a result, South Africa's cyberthreat landscape is expected to continue being diverse and complex. According to Watambwa (2021), security vulnerabilities within the public sector can have severe consequences for individuals, organizations, administrations, and governments. These vulnerabilities encompass a range of cyber threats, including identity theft, fraud, abuse, industrial espionage, and even potential terrorist activities, posing risks to public security and order.

2.4. Innovative solutions or frameworks for improving cybersecurity measures

In today's rapidly evolving digital landscape, innovative frameworks such as Zero Trust Architecture (ZTA) have emerged as pivotal

solutions for bolstering cybersecurity measures. ZTA operates on the principle of "never trust, always verify", ensuring that both external and internal traffic is monitored and authenticated before being granted access to network resources. By integrating advanced technologies like artificial intelligence (AI) and machine learning (ML), organizations can enhance threat detection and response capabilities, effectively mitigating risks posed by sophisticated cyberattacks. Furthermore, the implementation of Secure Access Service Edge (SASE) combines networking and security into a unified cloud service, providing seamless, secure connections for remote workforces. The adoption of decentralized cybersecurity frameworks, such as blockchain for identity verification, is also gaining traction, as it offers a tamper-proof mechanism for managing access and enhancing data integrity. Collectively, these frameworks not only strengthen an organization's security posture but also adapt to the complexities of modern threat environments (Cybersecurity & Infrastructure Security Agency [CISA], n.d.).

3. RESEARCH METHODOLOGY

This study adopted a quantitative research approach to examine the effectiveness of local authorities' cybersecurity policies in preventing and detecting fraud. Data were collected through structured questionnaires, ensuring the systematic gathering of responses from the target population of 160 participants, including employees, managers, and supervisors. A sample of 80 participants was selected for the administration of questionnaires, using simple random sampling to ensure each member of the target population had an equal chance of selection. Data analysis was carried out utilizing SPSS version 23, which provided tools for descriptive and inferential statistics, thus allowing for the quantification of relationships between various factors related to cybersecurity policy effectiveness (Field, 2013). Quantitative methods were appropriate for this study as they facilitate the identification of patterns and trends in responses, which can be analyzed for statistical significance.

Alternative methods that could also be suitable for conducting this research include qualitative approaches such as interviews or focus groups. Qualitative methods would allow for a more in-depth exploration of participants' experiences and perceptions regarding cybersecurity policies, potentially uncovering nuanced insights that quantitative methods might overlook (Creswell, 2014). For instance, semi-structured interviews could be used to gather detailed narratives from a diverse range of stakeholders within local authorities, providing a rich understanding of the challenges and effectiveness of current cybersecurity measures. Additionally, a mixed-methods approach could be employed, combining quantitative surveys with qualitative interviews to create a more comprehensive understanding of the impact of cyberthreats on financial integrity. This approach would enable triangulation of data, enhancing the validity and reliability of the findings (Creswell & Plano Clark, 2011).

Table 1. Composition of population and sample size of questionnaire respondents

Local authority	*Target population*	*Questionnaire*
Masvingo City Council	50	30
Masvingo Rural District Council	30	15
Chiredzi Town Council	35	20
Gutu Rural District Council	45	15
Total	160	80

Source: Primary data, 2023.

4. RESULTS

4.1. Cyberthreats in local authorities

Table 2 captures the responses of participants regarding the prevalence of cyberthreats within local authorities. The table summarizes the level of agreement among respondents to the statement, "*There are cyber threats in local authorities*". By categorizing the responses into three distinct groups, strongly agree, agree, and neutral, we can analyze the overall perception of cybersecurity risks faced by these institutions. This analysis not only reveals the extent of awareness among local authority officials but also serves as a critical indicator of their preparedness to address such threats. Ultimately, examining these perceptions will aid in evaluating the effectiveness of current cybersecurity policies and highlight potential areas for improvement.

Table 2. Cyberthreats in local authorities

Responses		*Frequency*	*Percent*	*Valid percent*	*Cumulative percent*
Valid	Strongly agree	42	58	58.3	58.3
	Agree	29	40.3	40.3	98.6
	Neutral	1	1.4	1.4	100.0
	Total	72	100.0	100.0	

Source: Authors' elaboration using SPSS version 23.

Table 2 shows that respondents agreed that local authorities in Masvingo Province are exposed to cyberthreats as shown by 58% of the respondents who strongly agree that the local authorities, they are employed by, are indeed exposed to cyberthreats followed by 40.3% who agreed.

4.2. Cyberattacks in local authority

To understand the prevalence of cyberattacks among local authorities in Masvingo Province, Table 3 presents a summary of participant responses regarding their experiences and perceptions of such incidents. The table illustrates a range of responses that highlight the extent to which individuals believe cases of cyberattacks have occurred within their respective local authorities. By categorizing responses into strong agreement and agreement, Table 3 allows for an analysis of differing opinions on the effectiveness of current cybersecurity measures. Additionally, the findings may indicate a potential gap in awareness or reporting of cyber incidents among local officials. Overall, this table serves as a critical component in assessing the state of cybersecurity and fraud detection within the local governance framework in Masvingo Province.

Table 3. Cases of cyberattacks in local authorities

Responses		*Frequency*	*Percent*	*Valid percent*	*Cumulative percent*
Valid	Strongly agree	44	61.1	61.1	61.1
	Agree	28	38.9	38.9	100.0
	Total	72	100.0	100.0	

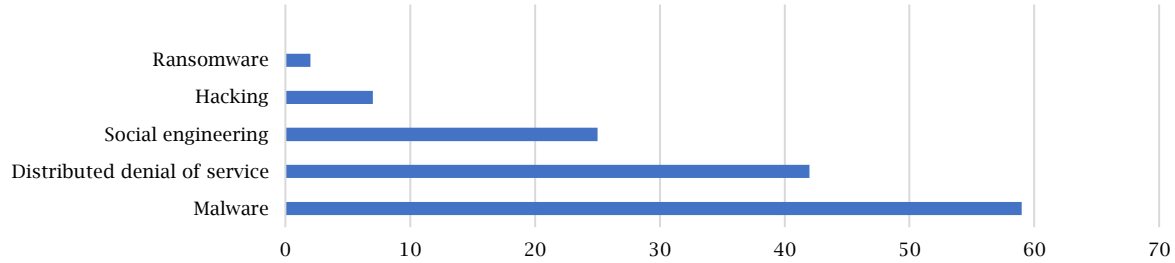
Source: Authors' elaboration using SPSS version 23.

Table 3 shows that all the respondents concurred that local authorities in Masvingo Province encountered cyberattack as shown by 61.1% who strongly agree with the remaining 38.9% agreeing that their organization encountered cyberattack. The results are supported by Li (2021), who found that 27.7% of the respondents reported that local authorities in the USA are attacked at least hourly, and another 19.4% reported being attacked at least once a day in the USA local authorities.

4.3. Cyberattacks faced by local authorities

Figure 1 outlines the various types of cyberattacks encountered by local authorities. It categorizes the attacks based on their prevalence and impact on financial integrity, providing a comprehensive overview of the threats faced in the digital landscape. The data compiled reflects the responses from various local authority representatives and highlights the most common vulnerabilities exploited by cybercriminals. By identifying these cyberattack types, we can better understand the specific challenges local authorities confront and assess the effectiveness of their existing cybersecurity policies. Ultimately, this analysis serves as a foundation for evaluating the ability of local authorities to prevent and detect fraud resulting from these cyberthreats.

Figure 1. Cyberattacks faced by local authorities



Source: Authors' elaboration using SPSS version 23.

Figure 1 shows that malware infection with 59% led as one of the cyberattacks faced by local authorities in Masvingo Province, Zimbabwe. According to Preis and Susskind (2022), local authorities in Poland are mainly vulnerable to spam, phishing, and malware. Their research produced that 47% of respondents agreed that local authorities have been attacked by spam, while 26.5% were attacked through phishing and 26.5% through malware.

4.4. Availability of written cybersecurity policy

Table 4 analyzes the availability of cybersecurity policies among local authorities, focusing on participants' perceptions regarding their effectiveness in preventing and detecting fraud. Table 4 summarizes responses from the participants who were asked to indicate their level of agreement or disagreement with specific statements related to the adequacy of existing policies. By capturing a range of opinions, this analysis aims to highlight areas of strength as well as shortcomings in the current cybersecurity framework. The findings illustrated in Table 4 provide valuable insights into the perceived robustness of these policies and their alignment with best cybersecurity practices. Ultimately, this information serves as a foundation for evaluating the overall impact of local authorities' cybersecurity measures on financial integrity.

Table 4. Analysis of availability of cybersecurity policy

Responses		*Frequency*	*Percent*	*Valid percent*	*Cumulative percent*
Valid	Strongly agree	16	22.2	22.2	22.2
	Agree	12	16.7	16.7	38.9
	Disagree	31	43.1	43.1	81.9
	Strongly disagree	13	18.1	18.1	100.0
	Total	72	100.0	100.0	

Source: Authors' elaboration using SPSS version 23.

Table 4 shows that most of the respondents disagree that their organizations have a written cybersecurity policy as illustrated by cumulatively 61.2% of respondents who strongly disagree and disagree that local authorities in Masvingo Province have cybersecurity policy compared to only cumulatively 38.9% who strongly agree and 22.2% who agree that the local authority they are employed by have written cybersecurity policy.

4.5. Effectiveness of cybersecurity policy

Table 5 presents the results of a survey conducted among participants regarding the effectiveness of their cybersecurity policies in preventing cybercrimes. The table categorizes responses into distinct groups, strongly agree, agree, neutral, disagree, and strongly disagree, offering a comprehensive overview of participants' perceptions. This quantitative analysis serves to

highlight the prevailing attitudes toward the adequacy of current cybersecurity measures within local authorities. By examining these findings, we aim to identify gaps in policy effectiveness and discern areas that may require further attention or improvement to enhance financial integrity and reduce vulnerability to cyberthreats.

Table 5. Effectiveness of cybersecurity policy in preventing cybercrimes

Responses		*Frequency*	*Percent*	*Valid percent*	*Cumulative percent*
Valid	Do not have a cybersecurity policy	44	61.1	61.1	61.1
	Strongly agree	12	16.7	16.7	77.8
	Agree	5	6.9	6.9	84.7
	Neutral	8	11.1	11.1	95.8
	Disagree	3	4.2	4.2	100.0
	Total	72	100.0	100.0	

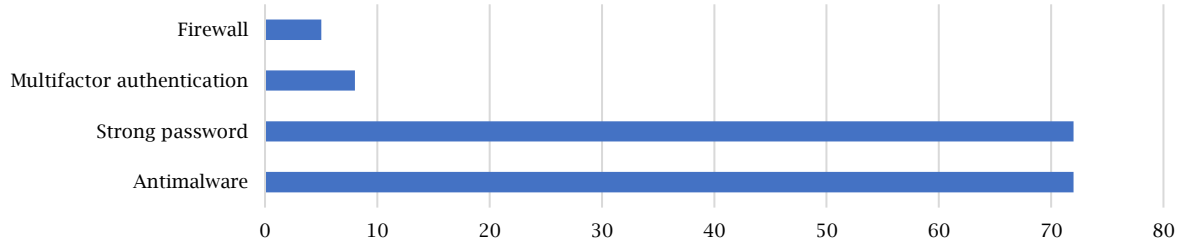
Source: Authors' elaboration using SPSS version 23.

Table 5 shows that a large portion of respondents represented by 61.1% asserted that their organizations do not have a written cybersecurity policy, and for the remaining percentage cumulatively 95.8% agree to strongly agree that their organization's cybersecurity policy is effective in preventing and detecting cybercrimes. This view is supported by Wadesango et al. (2024), who put forward that for cybersecurity policy to be effective, there should be meaningful metrics to be quantified in terms of time, money, and or risk level.

4.6. Cybersecurity appliances in local authorities

Figure 2 presents a comprehensive overview of the various types of cybersecurity appliances utilized by local authorities to enhance their defenses against cyberthreats. This analysis categorizes these appliances based on their specific functionalities, including firewalls, intrusion detection systems, and endpoint protection solutions. By examining the prevalence and effectiveness of these tools, we gain valuable insights into the current state of cybersecurity practices among local authorities and their impact on preventing and detecting fraud.

Figure 2. Types of cybersecurity appliances used in local authorities: Masvingo Province



Source: Authors' elaboration using SPSS version 23.

Figure 2 shows that most respondents agreed that cybersecurity appliances in the form of antimalware software, strong passwords are mainly used to prevent and detect cyberattacks. The results are further supported by Choi (2021), where respondents agreed that local authorities in the USA use antivirus software, firewall, spam blockers, and filters mainly, with only 2.7% agreeing that local authorities in the USA use SIEM, 5.4% VOIP encryption and 7.8% early warning system.

4.7. Effectiveness of cybersecurity appliances in detecting cyberattacks

Table 6 presents the participants' responses regarding the effectiveness of cybersecurity appliances in preventing and detecting cyberattacks. This data highlights the varied perceptions among local authorities about their current cybersecurity measures and their capabilities in safeguarding financial integrity. Understanding these viewpoints is critical for evaluating the overall impact of existing policies and identifying areas that require improvement or further investment.

Table 6. Effectiveness of cybersecurity appliances in preventing and detecting cyberattacks

Responses		*Frequency*	*Percent*	*Valid percent*	*Cumulative percent*
Valid	Strongly agree	13	18.1	18.1	18.1
	Agree	16	22.2	22.2	40.3
	Neutral	9	12.5	12.5	52.8
	Disagree	34	47.2	47.2	100.0
	Total	72	100.0	100.0	

Source: Authors' elaboration using SPSS version 23.

Table 6 shows that out of 72 respondents, 47.2% disagreed that their organizations' cybersecurity appliances are effective to prevent and detect cyberattacks and cumulatively 18.1% agree to strongly agree that their cyber security appliance is effective in preventing and detecting cyberattacks. The results are the opposite of Watambwa's (2021) survey where 96.3% of respondents agree that local authorities' antivirus is effective, 89% agreed that local authorities' firewall is effective in preventing cyberattacks, with 69.2% agreeing that Spam blockers and filters are effective in preventing and detecting cyberattacks.

4.8. Availability of cybersecurity mitigation training in local authorities

Table 7 presents the responses from participants regarding the availability of cybersecurity mitigation training within local authorities. The aim is to gauge perceptions of whether such training is adequately provided to enhance cybersecurity awareness and capabilities among employees. Understanding the level of agreement or disagreement on this matter is crucial for evaluating the effectiveness of local authorities' cybersecurity policies in preventing and detecting fraud.

Table 7. Undertaking of cybersecurity mitigation training

Responses		*Frequency*	*Percent*	*Valid percent*	*Cumulative percent*
Valid	Strongly agree	3	4.2	4.2	4.2
	Agree	7	9.7	9.7	13.9
	Neutral	3	4.2	4.2	18.1
	Disagree	42	58.3	58.3	76.4
	Strongly disagree	17	23.6	23.6	100.0
	Total	72	100.0	100.0	

Source: Authors' elaboration using SPSS version 23.

Table 7 shows that a total of 81.9% of respondents strongly disagreed and disagreed that local authorities in Masvingo Province undertake cybersecurity mitigation training and only 13.9% strongly agreed that local authorities they are employed by undertake cybersecurity mitigation training. The results contrast with Preis and Susskind (2020), who found out from the survey they carried out that 51.5% of municipalities in Poland undertake cybersecurity mitigation training and 49.5% of municipalities in Poland failed to engage in cybersecurity mitigation training due to lack of funds to finance such cybersecurity mitigation training.

4.9. Categories of employees who undertake cybersecurity mitigation training in local authorities in Masvingo Province

Table 8 presents an analysis of the categories of employees who participate in cybersecurity mitigation training within local authorities. It categorizes employees based on their roles, highlighting the varying levels of training received and the significance of each role in the context of cybersecurity. This analysis aims to assess how well these training initiatives are aligned with the specific responsibilities of different employee categories, thereby evaluating their effectiveness in enhancing the organization's overall cybersecurity posture.

Table 8. Analysis of categories of employees who undertake cybersecurity mitigation training

Responses		*Frequency*	*Percent*	*Valid percent*	*Cumulative percent*
Valid	Do not engage in cybersecurity mitigation training	62	86.1	86.1	86.1
	Management	7	9.7	9.7	95.8
	Supervisors	3	4.2	4.2	100.0
	Total	72	100.0	100.0	

Source: Authors' elaboration using SPSS version 23.

Table 8 shows that 86.1% of the respondents who work for the local authorities answered by "do not engage in cybersecurity mitigation training" and respondents who agree that their organizations engage in cybersecurity mitigation training agreed that such cybersecurity mitigation training is received only by management and supervisors while officers do not receive cybersecurity mitigation training.

4.10. Effectiveness of local authorities' cybersecurity mitigation training in preventing cybercrimes

Table 9 presents the results of a survey conducted among local authority staff regarding their perceptions of the effectiveness of cyber mitigation training programs. Participants were asked to express their level of agreement or disagreement with various statements related to the training's impact on enhancing cybersecurity awareness and skills. The data aims to highlight the perceived effectiveness of these training initiatives in preventing and detecting fraud-related cyber threats within local authorities.

Table 9. Effectiveness of cybersecurity mitigation training

Responses		*Frequency*	*Percent*	*Valid percent*	*Cumulative percent*
Valid	Do not engage in cybersecurity mitigation training	61	84.7	85.9	85.9
	Strongly agree	6	8.3	8.5	94.4
	Agree	4	5.6	5.6	100.0
	Total	71	98.6	100.0	
Missing	System	1	1.4		
Total		72	100.0		

Source: Authors' elaboration using SPSS version 23.

Table 9 indicates that out of 72 respondents cumulatively only 14.1% agreed and strongly agreed that cybersecurity mitigation training is one of the effective techniques in preventing and detecting cybercrimes in local authorities in Masvingo Province.

5. DISCUSSION

The findings indicate a significant vulnerability among local authorities in Masvingo Province, Zimbabwe, who face various cyberthreats including

malware, phishing, and distributed denial of service attacks. This aligns with the broader trend observed globally, where local government entities are increasingly targeted due to their often outdated and inadequate cybersecurity measures (Wadesango et al., 2023). The lack of a clearly defined cybersecurity policy among most local authorities, except for the Masvingo Municipal Authority's recent initiative, highlights a critical gap in governance that can exacerbate exposure to cyber threats (Watambwa, 2021). Research has shown that a well-structured cybersecurity policy is vital for establishing a proactive defense against attacks, with its effectiveness greatly enhanced by regular audits and updates to address evolving threats (Choi, 2021). Moreover, the limited scope of cybersecurity mitigation training largely targeting only management and supervisors suggests a need for a more holistic approach that includes all personnel, as human error remains a prominent factor in cyber vulnerabilities (Hubbard, 2019). Comprehensive training for all staff is essential, as a culture of cybersecurity awareness can significantly reduce the risk of successful attacks (Li, 2021). In conclusion, local authorities in Masvingo Province must adopt more rigorous cybersecurity policies that not only emphasize preventive measures but also foster an organization-wide culture of security mindfulness to safeguard financial integrity.

6. CONCLUSION

This study highlights significant vulnerabilities within local authorities in Masvingo Province, Zimbabwe, regarding their exposure to cyberthreats. The findings indicate that these authorities face various cyberattacks, including malware infections, DDoS attacks, and phishing attempts. Alarmingly, most local authorities lack comprehensive cybersecurity policies, except for Masvingo Municipal Authority, which has recently attempted to institute such a framework. This absence of clearly defined policies underscores a critical gap in the strategic response to cyber threats, ultimately jeopardizing financial integrity and the security of public resources.

The implications of these results are profound. The existence of an effective cybersecurity policy is crucial for mitigating cyberthreats and ensuring timely detection of cyberattacks. Moreover, the study reveals that while some local authorities engage in cyber mitigation training, the focus primarily remains on management and supervisory levels, leaving operational staff and other personnel potentially ill-prepared for cyber incidents. To strengthen cybersecurity resilience, it is vital for local authorities to invest in comprehensive training programs that encompass all levels of staff and to implement regular audits of their cybersecurity policies to foster continuous improvement and adapt to evolving threats.

However, this research is not without limitations. The study's scope was confined to local authorities within Masvingo Province, which may not fully represent the cybersecurity landscape across Zimbabwe as a whole. Future research should expand to include a broader range of local authorities and potentially explore the impact of international best practices in cybersecurity policy implementation. Furthermore, a longitudinal study could provide insight into the effectiveness of newly implemented policies over time and assess how local authorities evolve their strategies in response to emerging cyber threats. Establishing robust frameworks for assessing cybersecurity maturity will be essential for securing the financial integrity of local governance in Zimbabwe.

REFERENCES

Choi, K. (2021). The driving force behind cybercrime: Cyber resilience and cybercriminology. *Journal of Contemporary Criminal Justice, 37*(3), 308–310. https://doi.org/10.1177/10439862211001631

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608. https://doi.org/10.2307/2094589

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). SAGE Publications.

Creswell, J. W., & Plano Clark, V. L. (2011). *Designing and conducting mixed methods researc*h. SAGE Publications.

Cyber terrorists target ZEC. (2022, November 15). *The Herald*. https://www.herald.co.zw/cyber-terrorists-target-zec/

Cybersecurity & Infrastructure Security Agency (CISA). (n.d.). *Zero trust maturity model*. https://www.cisa.gov/zero-trust-maturity-model

Deda, G., Tërstena, A., Krasniqi, S., & Todorova, S. (2024). Evaluation of influence of corruption, lending interest rate and other components on ease of doing business: A policy-making and legal implications. *Corporate Law & Governance Review, 6*(3), 8–16. https://doi.org/10.22495/clgrv6i3p1

Field, A. (2013). *Discovering statistics using IBM SPSS statistics* (4th ed.). SAGE Publications. https://sadbhavnapublications.org/research-enrichment-material/2-Statistical-Books/Discovering-Statistics-Using-IBM-SPSS-Statistics-4th-c2013-Andy-Field.pdf

Hubbard, J. (2019). SA business underplaying the danger of cybercrime? *Finweek, 2019*(4), 37–38. https://hdl.handle.net/10520/EJC-1444bed59d

Ifere, E. O., Ovat, O. O., Owan, E. J., Chijioke, M. I., Ofem, L. U., Ndome, J. N., Ugbaka, M. A., & Atelhe, A. G. (2023). Perception and criminality of tax evasion in a developing economy [Special issue]. *Corporate Law & Governance Review, 5*(2), 164–173. https://doi.org/10.22495/clgrv5i2sip3

Karpiuk, M. (2021). The local government's position in the Polish cybersecurity system. *Lex Localis, 19*(3), 609–620. https://doi.org/10.4335/19.3.609-620(2021)

Li, J. (2021). Cybercrime in the Philippines: A case study of national security. *Turkish Journal of Computer and Mathematics Education (TURCOMAT),* 12(11), 4224–4231. https://turcomat.org/index.php/turkbilmat/article/view/6550

Marzuki, S., & Ali, M. (2024). Judicial ethics violations: Legal aspect and the role of judicial supervision. *Corporate Law & Governance Review, 6*(3), 17–26. https://doi.org/10.22495/clgrv6i3p2

Preis, B., & Susskind, L. (2022). Municipal cybersecurity: More work needs to be done. *Urban Affairs Review, 58*(2), 614–629. https://doi.org/10.1177/1078087420973760

Reserve Bank of Zimbabwe (RBZ). (2020). *2020 Annual report*. https://www.rbz.co.zw/index.php/publications-notices/publications/annual-reports/744-2020-annual-report

Rozah, U., & Pujiyono. (2022). Governance and regulation of aligning ISO 37001 in mitigating corporate bribery risks. *Corporate Law & Governance Review, 4*(2), 17–26. https://doi.org/10.22495/clgrv4i2p2

Sheehy, B., & Madrid, K. G. L. (2022). Convergence of corporate governance in state-owned enterprises: A case study in an emerging market using OECD Guidelines. *Corporate Law & Governance Review, 4*(1), 19–34. https://doi.org/10.22495/clgrv4i1p2

The Office of the Auditor-General of Zimbabwe. (2020). *Report of the Auditor-General on the local authorities*. https://www.auditorgeneral.gov.zw/downloads/category/4-local-authorities?download=47:ag-report-2020-on-local-authorities

Wadesango, N. (2024). The role of information technology systems (IT) on the development of effective internal controls. Desktop study. *Journal of Economic and Social Development (JESD) — Resilient Society, 11*(2), 126–139. https://www.jesd-online.com/articles/the-role-of-information-technology-systems-it-on-the-development-of-effective-internal-controls-desktop-study.pdf

Wadesango, N., Nasoma, D., & Sitsha, L. (2024). Effectiveness of auditor's report as a medium of communication to reduce the level of the audit expectation gap of Amon Chartered Accountants. *CECCAR Business Review, 2024*(7), 62–73. https://doi.org/10.37945/cbr.2024.07.07

Wadesango, N., Ruwende, J. W., & Sitsha, L. (2023). Evaluating the impact of financial management practices on an organization's financial performance: A case study of Hwange Colliery Company. *International Journal of Economics and Financial Issues, 13*(6), 203–208. https://doi.org/10.32479/ijefi.14275

Watambwa, L. (2021). *Cybercrime in local authorities: A case study of the Bulawayo City Council*. https://doi.org/10.2139/ssrn.3779482

Zimdef suffers a $120 million loss as a result of bank account hacking. (2023, January 8). *Zim Morning Post*. https://zimmorningpost.com/zimdef-suffers-a-120-million-loss-as-a-result-of-bank-account-hacking/