ASSESSMENT OF ZIMBABWE'S CYBERSECURITY READINESS AND INFRASTRUCTURE

AFRICA UNIVERSITY A UNITED METHODIST-RELATED UNIVERSITY

2025

AFRICA UNIVERSITY

(A United Methodist Related Institution)

ASSESSMENT OF ZIMBABWES CYBERSECURITY READINESS AND INFRASTRUCTURE

BY

TAMPIWA MAHARI

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF BACHELORS IN COMPUTER SCIENCE IN THE COLLEGE OF ENGINEERING AND APPLIED SCIENCES

2025

Abstract

The purpose of this research was to evaluate Zimbabwe's Cybersecurity readiness and infrastructure, focusing particularly on the synergy on the integration of adequate cybersecurity measures withing organizational frameworks. The study is undertaken against a backdrop of rising cyber threats targeting multiple sectors. Cyber threats, such as data breaches, highlight weaknesses that are brought to surface from technological deficiencies, limited awareness and lack of policy enforcement. This research focuses on the problems organizations confront in their cybersecurity readiness, exploitations cybersecurity infiltrates in the technological gaps. Relevant literature highlighted the critical gaps, such as inadequate training, outdated IT infrastructure and weak legislative frameworks, which obstruct Zimbabwe's ability to act upon modern cyber threats effectively. Questionnaires were the primary tool used to collect data, designed to gather quantitative and qualitative perceptions across various organizations. The questionnaire included a combination of Likert-scale items, leading questions and dichotomous questions to assess cybersecurity challenges, policies and practices. The findings were represented though graphs for clarity and easy of interpretation. The findings revealed a significant proportion of organizations are unprepared to deploy appropriate cybersecurity measures. Based on the research findings, emphasis was placed on all sectors adopting cybersecurity prioritization. Basing off of the rising targeting of key sectors of the nation, the research emphasizes the need for the government to finalize and implement the National Cybersecurity Policy. The recommendations outlined in this study aim to provide actionable strategies for various stakeholders to mitigate cyber risks and strengthen Zimbabwe's overall cyber security infrastructure.

Keywords

Cybersecurity, Cyber threats, Information security, Cyber resilience, Cyberattack

Declaration

I, hereby declare that this research study titled "Assessment of Zimbabwe’s Cybersecurity Readiness and Infrastructure" is the result of my own original work. All ideas, concepts, data, and insights presented in this project are entirely my own, except where explicitly stated otherwise.

TAMPIWA MAHARI **T.L. Mahari**

Students Full Name **Students Signature 28/03/2025**

LOVELY TEMBANI-FUNDISI

Main Supervisors Full Name **Main Supervisors Signature 28/03/2025**

Copyright

Acknowledgement

I am deeply grateful to my supervisor, Mrs L Tembani-Fundisi, for her continued guidance, encouragement and support throughout this research. Her feedback and insight were essential in shaping this study.

I extend my gratitude to the participants that assisted in my research by investing their time and perspectives.

Finally, I would like to extend my gratitude to Africa University, College of Engineering and Applied Sciences, for providing me with the necessary resources to make this study a success.

Dedication

I would like to express my deepest gratitude to my mother, Moyra Mahari, for her continuous unwavering support. Her belief in me has been a constant motivation and a source of strength. She is my greatest inspiration and my constant reminder that you can overcome any obstacle with perseverance and faith.

To my uncles, aunt, and Sisters, I owe a debt of gratitude for their encouragement and countless way they have supported me. Their words of motivation have been a light in times of doubt.

Lastly, I wish to honour the memory of my late uncle, Dr Maxwell Mahari, whose passion for knowledge and excellence continues to inspire me to this day. Even though he is no longer with us I dedicate this work to him with a heartfelt appreciation.

List of Acronyms & Abbreviations

CS	Cyber Security
IT	Information Technology
CBD	Central Business District
ICT	Information and Communication Technology
POTRAZ	Postal and Telecommunications Regulatory Authority of Zimbabwe
RBZ	Reserve Bank of Zimbabwe
ZDI	Zimbabwe Democrats Institute

Table of Contents

List of Tables

List of Figures

CHAPTER 1 INTRODUCTION

1.1 Introduction

Cybersecurity is the practice of safeguarding digital systems, networks, and data from malicious attacks, unauthorized access, and data breaches (Grustniy, 2019), described Cyber Security as the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. The International Telecommunication Union (ITU, 2021) expands this definition to include "the collection of tools, policies, and technologies designed to protect the confidentiality, integrity, and availability (CIA triad) of information in cyberspace".

Cyber security is also acknowledged as the information technology (IT) security protecting software as well as hardware free of threats. Mehio (2019) argued that cyber security represents a complex socio-technical challenge faced by all the organizations in present day such as governments as well as private companies but requiring the involvement of individuals. Limited awareness and transparency make cybersecurity challenging for many people.

Globally, cybersecurity spending is projected to exceed $1.75 trillion by 2025 (Gartner, 2023), yet Sub-Saharan Africa, including Zimbabwe, accounts for less than 2% of this investment (ITU, 2023). This disparity underscores systemic vulnerabilities in regions with limited infrastructure and policy enforcement. For example, Zimbabwe's mobile money penetration reached 96% in 2024 (POTRAZ), but cybersecurity frameworks lag behind, leaving critical sectors like finance and healthcare exposed to ransomware and phishing attacks (Chikomba et al., 2023).

The increased use of technology and the digital sphere transforming the public sector, have resulted in a rise in cyber threats. Over and above that, the Covid-19 era promoted online or remote jobs which thereby exposed many vulnerabilities within the cyber space (Palmer, 2020). While the issue of cyber threats remains a challenge, there has been evidence in the increase in sophistication by the hackers who are formulating new ways for new targets daily (Guyas 2022). Many national technology initiatives do not currently prioritise cybersecurity, particularly in the majority of developing nations (James, 2017).

Initiatives related to cybersecurity are still in their infancy, particularly in developing nations like Zimbabwe. As a result, developing nations continue to have more challenges when implementing their cybersecurity, which increases the failure rate compared to developed nations. Since governments increasingly rely on the information stored and transferred across sophisticated communication networks, cybersecurity is essential for the effective adoption of the new technologies. This paper will present a review of the Cybersecurity readiness and infrastructure in Zimbabwe. The study will bring out some of the factors and provide recommendations on effective Cybersecurity and infrastructure practices.

1.2 Background of the study

In the late 1990s – 2000, majority of the computer-based cyber threats were in the form of computer worms and viruses that were primarily intended to gain notoriety for the malicious code author and to expose vulnerabilities of popular software and hardware makers just to embarrass them. Therefore, these sorts of problems made the job of the system security more of a technological problem that focused on vulnerabilities rather than on threats, which have eventually led to today's endless cycle of software updates and patches.

The Reserve Bank of Zimbabwe (RBZ, 2023) reported a 300% increase in banking-sector cyberattacks between 2020 and 2024, with losses exceeding $25 million annually. High-profile incidents, such as the 2024 ransomware attack on ZB Financial Holdings that exposed 500,000 customer records (TechZim, 2024), highlight the urgent need for modernized incident response protocols. Unlike regional peers like Kenya (Data Protection Act, 2021) and South Africa (POPIA, 2020), Zimbabwe's draft *Cybercrime and Cybersecurity Bill* (2013) remains unimplemented, exacerbating legal gaps.

The importance of technology therefore made management of information a lot easier although there is a gloomier aspect of this. With the world depending more and relying on information technology, businesses have become vulnerable to cyber-attacks and in the process lose their greatest asset which is information. It is against this background that cyber security readiness and infrastructure has been pointed to be one of the most essential prerequisites of information security behaviour and a key player in employees policy compliance.

With cyber space growing rapidly, about 3 billion people are now connected to the cyber space through the internet. This therefore brings to life the necessity of cyber security readiness and preparedness for organisations. According to Majome (2017), the then Ministry of ICTs, Postal and Courier Services in 2013 drafted the Cybercrime and Cyber security Bill in trying to make efforts to keep up with global trends, as it is now essential for all countries to come up with laws that classify and deal specifically with cybercrimes, without dedicated statutes, there will be no legal mechanisms on which to prosecute the cybercriminals. With the use of internet now, it is a place where most of the people are involved in all sorts of activities, hackers and cyber criminals find it as a place to do their operations and as such putting many companies at risk.

Many organisations hold sensitive data which they cannot afford to lose to hackers and with the diverse types of attacks that organisations are exposed to, it triggered the researcher to assess the cyber security readiness and infrastructure in Zimbabwe. Cybersecurity has become a priority for many institutions across the world, especially considering their responsibility of ensuring their citizens’ security (Martins, 2021). Although cybersecurity has become a priority for many governments around the world, various organisations are still under threat with a risk of cyber-attacks. Some of the private organisations invested in the development and invention of technological security solutions with specific focus on their cybersecurity.

Cyber-attacks are continuing in Zimbabwean public sector and on some of the private organisations due to inadequate cybersecurity skills and a lack of cyber awareness. Majority of the public have experienced continued financial decline due to poor cybersecurity. The impact of these have often resulted in ransomware attack and the affected institutions had to pay large amounts of ransom (Poll, 2020). Patrick (2019) pointed out a problem of information silos regarding cybersecurity in government agencies and the requirement for a response team.

1.3 Statement of the problem

The increase in technology globally made nations and organizations to be vulnerable to cyber-attacks. This caused nations to lose billions of dollars each year (Africa Cyber-Security Report, 2024). Developing nations encounter various obstacles in their efforts to thwart cyberattacks targeting their hardware and software infrastructure.

Many vulnerabilities exist in existing systems, and in technical infrastructure. There is a scarcity and inadequate cybersecurity services and outdated Information Technology infrastructure and insufficient cybersecurity user awareness education. Zimbabwean public sector still lacks the technical knowledge and skills to manage the cybersecurity attacks (Machaka, 2021). Notwithstanding the shortages or poor cybersecurity skills, there is also still the usage of old fashioned and ageing technological infrastructure as well as minimal pro-active cyber-security user awareness. Therefore, cyber-threats are continuing to worsen each year. The recent adoption of digital technologies and the usage of advanced technologies has resulted in increased attraction to hackers. The Zimbabwean public sector evidenced increase in cybersecurity attacks, which have resulted in reputational damage and financial losses. Therefore, it was crucial to assess the cybersecurity readiness and infrastructure to manage the cybersecurity.

1.4 Research Objectives

1. To determine major factors influencing cyber security readiness and infrastructure in Zimbabwe
2. To evaluate the effectiveness of Cybersecurity practices in Zimbabwe.
3. To identify strategies for improving Cybersecurity infrastructure in Government and Public institutions.

1.5 Research Questions

1. What are the major factors influencing cybersecurity readiness and infrastructure?
2. How effective are current cybersecurity practices in Zimbabwe?
3. What strategies can improve cybersecurity infrastructure in government and public institutions?

1.6 Assumption of the study

This study assumed that,

- All targeted respondents provided timely and accurate responses.

- The respondents who participated in this research study wanted to improve the cybersecurity readiness within the nation.
- The participants were honest in their responses.
- Participants were willing to provide responses about their cybersecurity readiness and infrastructure activities with reasonable assurance of anonymity and privacy.

1.7 Significance of the study

This study advanced the current study in the areas of cybersecurity readiness and infrastructure. As a result, the findings from this study contributed to the body of knowledge in the fields of cybersecurity management. Although literature had been published focusing on improvements in cybersecurity, a gap existed with respect to the readiness and infrastructure in Zimbabwe. Thus, this research study provided a benchmarking tool on improving the cybersecurity in the country. Additionally, this research study offered a cybersecurity planning program that could be used as a strategic guide to mitigate cyber-attacks and maintain business continuity.

1.8 Delimitation of the study

Delimitations are the constraints that have been anticipated and used to scope and establish boundaries for the respective research (Barbian, 2015). The population sample for this research study was taken from a specific area, which was the CBD of Harare. The interview population included IT professionals with knowledge of or experience in cybersecurity in critical infrastructure in Zimbabwe.

1.9 Limitation of the study

The study assessed Zimbabwe's cybersecurity readiness and infrastructure using primary data from 66 respondents across various sectors, including the private sector, public institutions, government agencies and academic organizations. The research was constrained by several factors, including the limited sample size, potential response bias and the scope of data collection, which focused primarily on organizational cybersecurity practices rather than an exhaustive national analysis. Additionally, the study relied on self-reported data, which may be subject to individual perception biases. Due to time and resource constraints, a more extensive investigation involving a larger sample and in-depth qualitative interviews could not be conducted.

CHAPTER 2 LITERATURE REVIEW

2.1 Introduction

The Merriam–Webster dictionary defines cybersecurity as “measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack” (Merriam-Webster, 2020). The International Telecommunications Union (ITU) defines cyber security as “the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets” within the cyber security foci of confidentiality, availability, and integrity (CIA) objectives (ITU, 2008).

Cyber Security Fast Facts
There were 2,365 cyberattacks in 2023, with 343,338,964 victims.
2023 saw a 72% increase in data breaches since 2021, which held the previous all-time record.
Around the world, a data breach cost $4.88 million on average in 2024.
Email is the most common vector for malware, with around 35% of malware delivered via email in 2023.
Ninety-four percent of organizations have reported email security incidents.
Business email compromises accounted for over $2.9 billion in losses in 2023.
Information security jobs are projected to grow by 32% between 2022 and 2032.

Table 1-Cybersecurity Fast Facts/https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/

Cybersecurity ideas and tactics differ across the board on an international scale, there is no universal way of handling cybersecurity as well as defining it in turn the Russian-US Bilateral working group of the East West Institute and Lomonsov Moscow State University developed a paradigm for terminology that described cyber security: “A property of cyber space that is an ability to resist intentional and unintentional threats and respond and recover” (ISI, 2014).

It is impossible to exaggerate the significance of cybersecurity in a world going more digital. The frequency of cybersecurity attacks is expected to continue rising as new and more sophisticated attacks are coming to light Herjavec (2019). The increasing reliance on digital technology across many industries underscores the need of protecting vital data and infrastructure from cyber-attacks.

Mukiibi (2019) reported that less than ten African countries have cybersecurity legislation. By 2022, 29 of the 54 African countries had cybersecurity legislation (Weforum, 2022). Like many other countries, Zimbabwe has enormous obstacles when it comes to tackling cybersecurity issues and making sure there is sufficient infrastructure and preparation to reduce possible dangers. Examining the literature, ideas, and empirical data relevant to Zimbabwe's cybersecurity environment is the goal of this review, which aims to evaluate the infrastructure and preparedness of the nation.

This chapter provided a review of existing literature on the subject of cybersecurity, with a key focus on the opportunities and challenges faced by Zimbabwe. Through exploration of the theoretical foundations, empirical studies and industry best practices. A strong foundation for the subsequent analysis and recommendations was established from this review.

2.2 Theoretical framework

Technology readiness, according to Parasuraman, is a personality attribute that can boost a person's acceptance of new technology for both personal and professional purposes. In the meantime, Chen, characterized technology readiness as a multi-asset construction that falls into two categories: components that promote technology adaptation and components that impede it. A measure of a person's readiness to adopt new technology can be their level of technological readiness (Chen, 2003).

Framework	**Zimbabwe**	**South Africa**	**Kenya**
Zero Trust	8%	42%	35%
NIST CSF	12%	67%	50%
ISO 27001 Certification	5%	58%	45%

Table 2- Security Tool Adoption vs. Regional Peers, ITU Global Cybersecurity Index (2023)

In Zimbabwe, discomfort (e.g., resistance to multi-factor authentication) and insecurity (e.g., fear of data breaches) dominate due to low digital literacy (ZDI, 2023). Modern frameworks like Microsoft’s Zero Trust Architecture (ZTA), which operates on the principle of 'never trust, always verify' (Microsoft, 2022), are absent in 92% of Zimbabwean organizations (PwC Zimbabwe, 2023). The U.S. NIST Cybersecurity Framework (NIST SP 800-207) offers a scalable template for Zimbabwe’s policy gaps, emphasizing Identify-Protect-Detect-Respond-Recover cycles.

Cybercrime

Cybercrime is escalating in Africa where it poses a challenge to the economic and social development of countries. Cybercrime, cyber espionage, cyber terrorism, and cyber warfare are all new types of cybercrime that pose a threat to African countries while ruthless cyber criminals such as hackers use cyber vulnerabilities to penetrate and destroy critical systems for financial gain or to hold user’s hostage (Peter, 2017).

Technology Readiness

The four sub-dimensions of technology readiness are optimism, innovation, discomfort, and insecurity. To investigate all the comprehensive elements that influence an organization's technological and cyber security preparedness as well as their simultaneous effects on performance, this study will develop a conceptual model. According to Eilts, no prior study has investigated small businesses' cyber security readiness or the relationship between organizational technology readiness and cyber security readiness and performance.

This study focused on cyber security readiness and infrastructure of organizations, assessing the impact of cyber security readiness and infrastructure readiness on security performance, tangible and intangible benefits in Zimbabwe. The difficulties and dangers associated with cybercrimes are ever-present threats to an organization's capacity to fulfil its mission and achieve its goals. Computer and communication security are included in cybersecurity (Wang et al., 2010). This entails controlling cyber risks related to an organization's computing and communication operations to a reasonable degree.

The strategic framework, business continuity, and governance of an organization all include the implementation of internet security risk management. In order to prevent cyberattacks and data breaches, it is the responsibility of organizations to make sure they are safeguarding the availability, integrity, confidentiality, and sensitive customer data while they are on the internet. Evaluating cyber security aids in determining how prepared a company is to identify, stop, and react to evolving online and cyberthreats (PwC, 2014).

The primary purpose of a cyber security readiness assessment is to help an organization visualize its current security posture and find any undiscovered vulnerabilities that need to be investigated and fixed. It is recommended that organizations periodically evaluate the security preparedness of their cyberspace systems to track advancements or possible regressions.

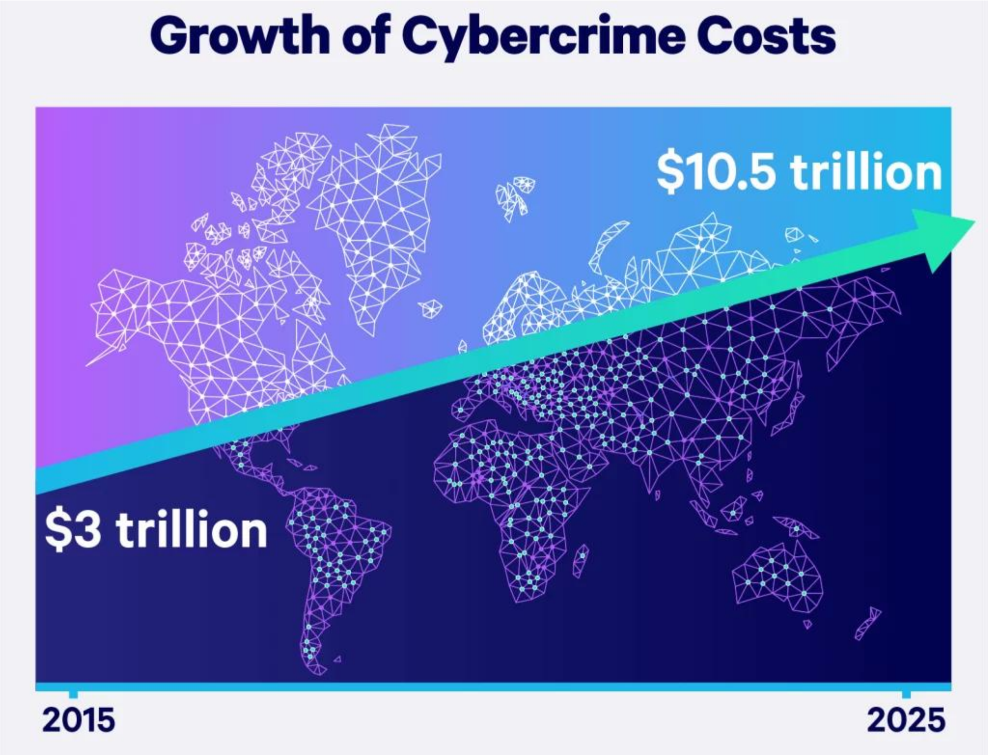


Figure 1-Costs of Cybercrime/https://www.embroker.com/blog/cyber-attack-statistics/

The first assumption would be cybercriminals are mostly targeting huge, trading companies. Whereas cyberattacks on smaller and medium sized businesses are rapidly on the rise, leaving some small businesses even more vulnerable and exposed. Whilst financial cost is a threat posed by cybercrimes; an organizations reputation can completely be tarnished as well as its long-term viability questioned.

Cyberattacks do range from targeted attacks on an individual through to larger organizations information technology systems. This can be carried out through the spread of viruses, malware, ransomware, and spam on users' devices through emails resulting in acquisition of sensitive information.

Global Cybersecurity Frameworks

Zimbabwe lags behind regional leaders in cybersecurity, but its shortcomings are similar to those of other developing countries. While Kenya's Data Protection Act (2021) required encryption for financial institutions, South Africa's implementation of AI-driven threat detection (Darktrace, 2023) decreased breaches by 40% (PwC East Africa, 2022). Zimbabwe's policy modernization can be modeled after the five fundamental roles of the NIST Framework: Identify, Protect, Detect, Respond, and Recover (NIST, 2021). Notably, 76% of Fortune 500 businesses currently utilize Zero Trust Architecture (ZTA) (Microsoft, 2022), which removes implicit trust in networks—a crucial necessity given the increase in insider threats in Zimbabwe (POTRAZ, 2023).

2.3 Relevance of the Theoretical Frame to the study

Zimbabwe’s Cybersecurity Landscape

According to Madondo (2017), one of the nations impacted by the rise in cybercrime and attacks is Zimbabwe. According to him, Zimbabwe's biggest problem is that it lacks cybersecurity, which leaves the country extremely open to cybercrime. He also mentions how cybercrime has become more prevalent in Zimbabwe because of the country's notable internet growth, with data from the Postal and Telecommunications Regulatory Authority of

Zimbabwe (POTRAZ) (2017) indicating a 50% penetration rate in 2016. Tatenda Mavetera, Minister of Information Communication Technology, POTRAZ (2024) said, “Zimbabwe is not immune to cyber threats, as evidenced by recent incidents where social media accounts of prominent individuals and entities were hacked.”

However, Kabata (2018) disputes the idea that there is no cyber security in Zimbabwe, claiming that although various organizations are putting cyber security measures in place, these are insufficient, necessitating the development of a cyber security culture within organizations. Furthermore, he contends that one of the difficulties facing Zimbabwe's ICT sector is the absence of a framework to offer focus, direction, guidance, and a standardized method of addressing cyber security issues.

Zimbabwe has experienced multiple cyber security breaches affecting different organizations, the majority of which are government departments. Cybercrime is listed as one of the crimes contributing to the US$1, 8 billion estimated illicit proceeds generated from criminal activity annually in Zimbabwe, according to the Reserve Bank of Zimbabwe (RBZ) (2015).

The 2023 African Cyberthreat Assessment Report ranked Zimbabwe 28th out of 54 nations in cybersecurity readiness, citing:

1. **Legislative delays:** No dedicated cybercrime law despite draft bills since 2013.

2. **Skills shortage:** Only 200 certified cybersecurity professionals serve 16 million people (POTRAZ, 2024).
3. **Outdated infrastructure:** 78% of public-sector entities use unsupported Windows 7 systems (Zimbabwe ICT Ministry, 2023). A 2023 phishing campaign impersonating ZIMRA stole $2.3 million via fraudulent tax emails, exposing gaps in public awareness and email filtering (The Herald, 2024)."

According to RBZ (2015), out of the 140 cybercrimes that were reported, 20 involved phishing, 13 involved credit card fraud, 10 involved identity theft, 24 involved unauthorized access, 72 involved hacking, and one involved telecommunications piracy. Zimbabwe's susceptibility to computer and cybercrimes is demonstrated by these statistics, underscoring the urgent need for organizations to be well-prepared. Njanjamangezi (2014) reports that Astro Mobile CEO Munyaradzi Gwatidzo concurs that Zimbabwe lacks adequate cyber security preparation, stating that over 90% of the country's organizations face cyber security threats.

Recent Cybersecurity Trends and Case Studies

Cybersecurity attacks have risen exponentially,
with emerging nations now being the target of choice for cybercriminals. In Zimbabwe, some of the most prevalent cybersecurity attacks are financial sector scams, unauthorized data breaches in the government, and phishing scams against businesses and individuals.

One such high-profile case that has occurred in recent times is that of ZB Financial Holdings, a giant Zimbabwean bank, which was attacked by a ransomware group in July 2024. The attackers stole files and offered to release them if a ransom was paid. When ZB refused, hackers dumped gigabytes of customer and operational data onto the dark web. Accounts indicate that data breaches included files dating back to 2017, including customer, employee, and account application details.

The attack was discovered by cybersecurity monitoring firms and made public through social media. The hackers, a group named “Mad Liberator”, targeted six victims across different regions, including South Africa, the UK, Spain, and Italy. The ZB Holdings attack highlights the vulnerability of Zimbabwe’s financial sector and the growing need for stronger cybersecurity measures.

This breach also raises incident response and transparency concerns. ZB Holdings did not issue an official statement to the media for inquiries even after the fact was known publicly, showing inadequate preparedness to deal with public communication in the wake of cyber-attacks.

Challenges and Opportunities

To stop cybercrime and have laws that permit prosecution of those who violate the law, the Ministry of ICTs, Postal and Courier Services began drafting the Cybercrime and Cybersecurity Bill in 2013, as Madondo (2017) points out. Majome (2017), on the other hand, disagrees with Madondo regarding the intent of the bill, contending that the Zimbabwean government had hidden agendas when drafting the bill, which was intended to violate citizens' rights and guarantee the government's control over the populace and their speech.

The Cybercrime Bill's intended goal, according to the Zimbabwe Democrats Institute (ZDI) (2018), was to criminalize social media misuse and grant the government more authority to interfere and monitor citizens' activities. As a result, it pays little to no attention to the necessity of upholding individual freedoms or holding people accountable for their actions when battling cybercrime.

The absence of a clear intention to protect fundamental human rights, as stated by the ZDI (2018), gives rise to concerns that the Cybercrime Bill was designed only to restrict internet use at the expense of people's freedom. Majome (2017) goes on to say that the Cybercrime Bill has a negative effect on the human rights that Zimbabwean citizens are entitled to.

Zimbabwe, has experienced significant challenges in the recent decades in the economic and political sectors, these challenges have seen a surge on the impact they have on the overall development of the country, the cybersecurity landscape is no exception. The world on a larger scale becomes increasingly interconnected through digital technologies, the need for robust cybersecurity

measures has become of high concern for nearly every nation across the globe, Zimbabwe being of no exception.
The administration of digital records in Zimbabwe’s financial services parastatals, which are government-owned entities, has presented a substantial obstacle.

The surge of information and communication technologies in the conduct of business has led to an increase in the generation of digital records, which are crucial for day-to-day business activities. However, the effective management of these digital records has been a persistent issue for most public sector institutions in Zimbabwe (Chikomba et al., 2020). This hurdle has left these records exposed to cyberattacks in turn affecting the nation’s overall cybersecurity posture.

In September of 2024, the government took a stride in cybersecurity practice as over a hundred government officials completed a new cybersecurity training program, which covered security trends, standards, governance and enterprise data security issues. Speaking at the graduation POTRAZ Deputy Director General, Mr Alfred Marisa said, “As we stand in an era where data has become the most valuable commodity it is essential that we recognise the importance of partnerships.

The global landscape has changed drastically with the amount of data consumed in 2023 doubling the previous years this has ushered in a new world order making cyber security a critical aspect of our digital lives. Our

> duty as public servants is to stay ahead of the curve ensuring that our digital infrastructure is not only functional but resilient against the ever-evolving trends we face.” (Fungai Jachi. 2024)

Summary

Africa loses over four billion USD annually to cybercrime; other critical losses include data, intellectual property, reputation, and brand name (Weforum, 2022). The implementation and integration of cybersecurity systems, particularly in Zimbabwe, are affected by cybersecurity factors that have not been sufficiently addressed by previous research despite the increased interest in cybersecurity infrastructure and readiness in Zimbabwe. Even though cybersecurity surveys have been carried out in other developing nations, it is exceedingly challenging to extrapolate findings to the context of Zimbabwe.

CHAPTER 3 METHODOLOGY

3.1 Introduction

The study strategy, design, data collecting strategies, and analytical methodologies used in evaluating Zimbabwe's cybersecurity infrastructure and preparedness are described in the methodology portion of this dissertation. Through the use of a strict methodology, this study successfully met the research objectives by collecting trustworthy data, analysing important factors, and coming to useful results.

With the intention of using a variety of trustworthy, legitimate, and credible reports from the sampled public sector organizations, this study employed the content analysis research methodology. The non-probability sampling methodology with purposive sampling technique was used in this investigation.

3.2 The Research Design

Research design refers to the overarching strategy that guides the systematic collection, analysis, and interpretation of data to address a study's objectives (Creswell & Creswell, 2023). For this study, a qualitative content analysis approach was employed to evaluate Zimbabwe's cybersecurity readiness and infrastructure. This method was particularly suited to examining textual or documentary data (such as policies, reports, and survey responses) to identify patterns, themes, and gaps in existing frameworks (Schreier, 2018).

Content analysis was selected for its ability to synthesize publicly accessible data from diverse sources, including:

- Organizational cybersecurity policies (e.g., government reports, industry norms).
- Survey responses from IT experts across sectors (see Chapter 3.4).
- Secondary data (scholarly literature, POTRAZ reports, etc.).

This methodological approach allowed for a methodical analysis of Zimbabwe's cybersecurity environment, guaranteeing rigor through open coding practices and allowing for emerging themes that were indicative of the country's particular policy and infrastructure issues.

3.3 Population and sampling

The term "population" describes the whole set of people, groups, or objects that satisfy the requirements to be included in a study (Creswell & Creswell, 2023). IT professionals, cybersecurity specialists, and staff members from important Zimbabwean sectors (government, business, academic, and public organizations) who deal with or have an impact on cybersecurity infrastructure made up the target group for this study.

A non-probability purposive sampling technique was used for this study, which is typical in qualitative research when targeting participants with specialized knowledge or experience relevant to the study's objectives (Palinkas et al., 2015). Sampling is the process of choosing a subset of the population to represent the whole, guaranteeing feasibility while maintaining validity (Etikan et al., 2016).

The study's sampling strategy was determined by the practical limitations of evaluating cybersecurity preparedness in Zimbabwe as well as the study's goals. A non-probability purposive sampling strategy was used because of the exploratory and qualitative character of the study. Participants with firsthand knowledge of or expertise in cybersecurity, such as IT specialists from important industries (government, business, university, and public institutions), were guaranteed to be included using this approach. Non-probability sampling is commonly used in qualitative research to produce in-depth insights, despite the fact that it does not support statistical generalization (Saunders et al., 2019). Practical factors (such as accessibility and resource constraints) and thematic saturation—the point at which more data no longer produced novel patterns pertinent to the study's objectives—were combined to establish the final sample size of 66 respondents.

3.3.1 Sample Size

The study collected responses from **66 participants**, a sample size determined through practical and methodological considerations to ensure meaningful insights while working within research constraints.

Practical Factors

- **Target Audience**: The study focused on IT professionals, cybersecurity experts, and employees from key sectors (government, private, academia). Given the specialized nature of cybersecurity roles, a smaller but highly relevant sample was prioritized over a larger, less targeted group.

- **Resource Limitations**: Time, budget, and accessibility influenced the sample size. Wider distribution was challenging due to low response rates in organizational surveys.

Methodological Suitability

- **Data Saturation**: After analyzing responses, it was observed that key themes (e.g., lack of training, outdated infrastructure) repeated consistently beyond 50 responses, suggesting sufficient coverage.
- **Comparative Benchmarking**: Similar studies on cybersecurity readiness in developing economies often use samples between 50–100 participants, making this sample size acceptable for exploratory research.

Representation Considerations

- **Sectoral Distribution**: While the private sector dominated responses (48/66), efforts were made to include government (5), public sector (4), and academic (9) participants to ensure diverse perspectives.
- **Expertise Balance**: Respondents ranged from beginners (19.7%) to advanced (33.3%), capturing varied levels of cybersecurity awareness.

Limitations & Adjustments

- **Potential Bias**: The sample may overrepresent certain sectors. To mitigate this, findings were cross-checked with secondary data (e.g., national cybersecurity reports).
- **Generalizability**: While not statistically representative of all Zimbabwean organizations, the sample provides actionable insights for policymakers and businesses.

The sample size of 66 strikes a balance between depth and feasibility, offering valuable insights into Zimbabwe's cybersecurity readiness while acknowledging inherent constraints.

3.4 Data collection instruments

This study employed a **mixed-methods triangulation approach** to ensure comprehensive data validity and reliability. The following instruments were utilized:

1. **Online Surveys (Primary Data)**
   - **Tool:** Google Forms (selected for accessibility, cost-effectiveness, and real-time data aggregation).
   - **Target Respondents:** 66 IT professionals across Zimbabwe's public/private sectors (see Section 3.3 for sampling rationale).
   - **Design:**
     - **Likert-scale questions** (e.g., "Rate your organization's cybersecurity preparedness from 1 (very poor) to 5 (excellent)").
     - **Dichotomous questions** (e.g., "Does your organization have a cybersecurity policy? Yes/No").
     - **Open-ended questions** (e.g., "Describe the biggest cybersecurity challenge your organization faces").
   - **Pilot Testing:** Conducted with 5 IT professionals to refine clarity and eliminate ambiguities (results excluded from final data).
   - **Distribution:** Shared via LinkedIn, professional WhatsApp groups, and email lists of Zimbabwe's Computer Society (ZCS).
2. **Semi-Structured Interviews (Primary Data)**

Purpose: To contextualize survey findings with expert insights.

Participants: 5 cybersecurity officers (2 from banking, 2 from telecoms, 1 from government).

Protocol:

- Conducted via Zoom/Phone (30-45 mins each).
- Questions focused on:

  "How does your organization implement incident response protocols?"

  "What policy gaps hinder Zimbabwe's cybersecurity readiness?"

  Audio-recorded (with consent) and transcribed verbatim.

3. **Document Analysis (Secondary Data)**

Sources:

- Policy Documents: Draft Cybercrime and Cybersecurity Bill (2013), POTRAZ Annual Reports (2020–2024).
- Academic Literature: Peer-reviewed journals on African cybersecurity challenges.
- News Reports: Verified cyberattack case studies (e.g., ZB Financial breach, TechZim).

4. **Observational Field Notes**

Primary data was augmented through systematic observation of cybersecurity practices during a professional internship with Tendo Electronics, where the researcher had authorized access to assess security postures across client organizations.

Sample Characteristics:

- Ten (10) client organizations within Harare's commercial sector
- Composition : 60% Financial services SMEs, 40% retail enterprises
- Observation period: August/2024 to December/2024

Observation Protocol:

- Documented manifest security behaviors (e.g., authentication practices)
- Recorded visible security infrastructure (e.g., endpoint protection systems)
- Noted policy implementation gaps through:
    - Direct behavioral observation
    - Review of publicly-posted security protocols

Methodological Value:

These observations enabled:

1. Triangulation of self-reported survey data (Section 4.2)
2. Identification of implementation challenges (Section 4.4.2)

3.5 Data Collection Procedure

In order to ensure anonymity and broaden the sampling area, an online survey was created using Google Forms. A pilot test was then conducted to refine the survey's questions, which covered cybersecurity readiness and infrastructure. The survey was then distributed across various platforms, securely received responses, and was analysed both quantitatively and qualitatively to provide insights into Zimbabweans' cybersecurity landscape.

Phase 1: Instrument Development:

A structured **Google Forms questionnaire** was created with three sections:

- **Demographics**: Sector, role, experience level.
- **Cybersecurity Practices**: Policies, training, tools.
- **Open-Ended Feedback**: Suggestions for improvement.

Questions used **Likert scales (1–5)**, dichotomous (Yes/No), and short-answer formats.

Phase 2: Pilot Testing:

Survey tested with 5 participants to refine clarity and avoid bias.

Phase 3: Distribution:

Shared via LinkedIn, professional networks, and institutional emails. With inclusion criteria focused on those employed in sectors critical to cybersecurity (finance, telecoms and government).

Participants were recruited via:

- **Professional networks** (LinkedIn, Zimbabwe IT forums).
- **Institutional emails** to government agencies (POTRAZ), banks, and universities.
- **Snowball sampling**: Respondents referred colleagues.

The Google Form link was distributed with a cover letter explaining:

- Research objectives.
- Anonymity assurances (no names/IPs collected).
- Estimated time commitment.

Phase 4: Data Collection and Validation:

1. **Response Monitoring:**
    - Real-time tracking via Google Forms identified response rates (66 completed surveys).
    - Partial responses (e.g., abandoned surveys) were excluded.

Phase 5: Data Compilation and Storage:

1. **Secure Aggregation:**
    - Survey data was downloaded as CSV files and stored on password-protected drives.
    - Identifiers (e.g., email addresses) were removed to anonymize responses.
2. Ethical Safeguards:
    - Participants signed digital consent forms (see Appendix).

3.6 Analysis and organisation of data

The study employed a **dual analytical approach** to examine both quantitative and qualitative data, ensuring a comprehensive assessment of Zimbabwe's cybersecurity readiness.

Quantitative Analysis

1. **Descriptive Statistics**:
    - Numerical data from Likert-scale and closed-ended survey questions were analyzed using **frequencies and percentages**.
    - Key metrics included:
        - Adoption rates of cybersecurity measures (e.g., firewalls, training programs).

    - Confidence levels in organizational security (e.g., "47% somewhat confident").
- Results were visualized using **bar graphs, pie charts, and tables** for clarity.

2. Comparative Analysis:

Zimbabwe’s cybersecurity metrics (e.g., 48.5% mobile device encryption) were benchmarked against regional peers (e.g., Kenya, South Africa) using data from the ITU Global Cybersecurity Index (2023).

The Qualitative Analysis Method

Thematic Coding:
Thematic analysis was employed to examine the qualitative data gathered from open-ended survey questions and additional sources. The categorization and coding of responses was determined by insights, patterns, and recurrent themes.
Open-ended responses and interview transcripts were analyzed to identify recurring themes (e.g., "lack of policy enforcement," "training gaps"). Codes were grouped into categories (e.g., **Awareness, Infrastructure, Policy**).

To enhance the clarity and accessibility of the results, visual aids such as **tables**, **charts**, and **graphs** were utilized. These tools were instrumental in presenting complex data in an easily interpretable format, enabling stakeholders to grasp the significance of the findings at a glance. For instance:

- **Bar graphs** were used to illustrate demographic distributions (e.g., gender representation, sectoral distribution).
- **Pie charts** were employed to depict the frequency of cybersecurity training and the effectiveness of awareness initiatives.
- **Tables** summarized critical statistics, such as the prevalence of cybersecurity policies and protocols across organizations.

Case Studies:

Examining actual cybersecurity case studies, such as data breaches or cyberattacks directed against persons or organisations in Zimbabwe, provided insightful lessons about the unique difficulties and vulnerabilities that exist in Zimbabwe.

3.7 Ethical considerations

This study's ethical issues include a number of important areas. First and foremost, participant confidentiality and anonymity must be guaranteed. This is especially important in a delicate field like cybersecurity, where people might be reluctant to share personal experiences or practices. Procedures for obtaining informed permission shall be clearly defined, explaining the goals of the research as well as the methods for gathering, storing, and using participant data. Furthermore, measures were taken to reduce any possible risk of injury or anxiety for attendees, particularly when they talked about personal experiences with cyberattacks or security breaches. Additionally, subjectivity in the study was not allowed to occur during the gathering, processing, or analysing of the data.

3.8 Summary

This chapter outlined the research design, sampling methods, data collection procedure and ethical considerations. The methodology ensured reliable data collection for evaluating Zimbabwe's cybersecurity readiness and infrastructure. The study employed a mixed-methods approach, combining surveys and secondary data analysis to assess cybersecurity readiness. Google Forms was chosen for data collection due to its accessibility and ability to reach a broad respondent base. However, to mitigate response biases, the survey included validation questions to ensure data integrity.

Sampling bias was managed by ensuring diversity in respondents, covering government agencies, financial institutions, academic sectors, and private businesses. This approach ensured that findings represent a holistic view of Zimbabwe's cybersecurity landscape.

CHAPTER 4: FINDINGS

4.1 Introduction

This chapter presents the analysis of the collected data from 66 respondents working in and around various sectors in Zimbabwe. The data was gathered through a mixture of quantitative and qualitative methods outlined in Chapter 3, including surveys, interviews and secondary data sources. The analysis focuses on identifying and examining key factors contributing to the readiness of Zimbabwe's infrastructure cybersecurity readiness.

The findings are based on a deep analysis of responses collected through a Google Form questionnaire. This chapter further assessed the effectiveness of current cybersecurity measures in place, assessing the strengths and weaknesses of existing frameworks and their effectiveness against modern threats. The analysis considered challenges organizations face in implementing robust cybersecurity practices such as lack of resources, gaps in technical expertise and the evolution of cyber threats.

Furthermore, this section applied several criteria, putting a focus on participants' experience within the Cybersecurity space as well as with their current organization. This section examined participants cybersecurity behaviours, perceptions as well as knowledge. Variations in responses between IT employees and different sector department end users were examined to provide comparative insights.

4.2 Data Analysis

4.2.1 Demographic Analysis

For a clearer understanding of the respondent pool, a demographic analysis was conducted. This section unpacked the distribution of participants across various demographic categories, namely gender, sector and level of cybersecurity experience. With this information potential bias identification and limitations were easier to identify, while also making it possible to draw insights into the specific needs and challenges faced by different groups within Zimbabwe's cybersecurity community.

4.2.1.1 Gender Representation:

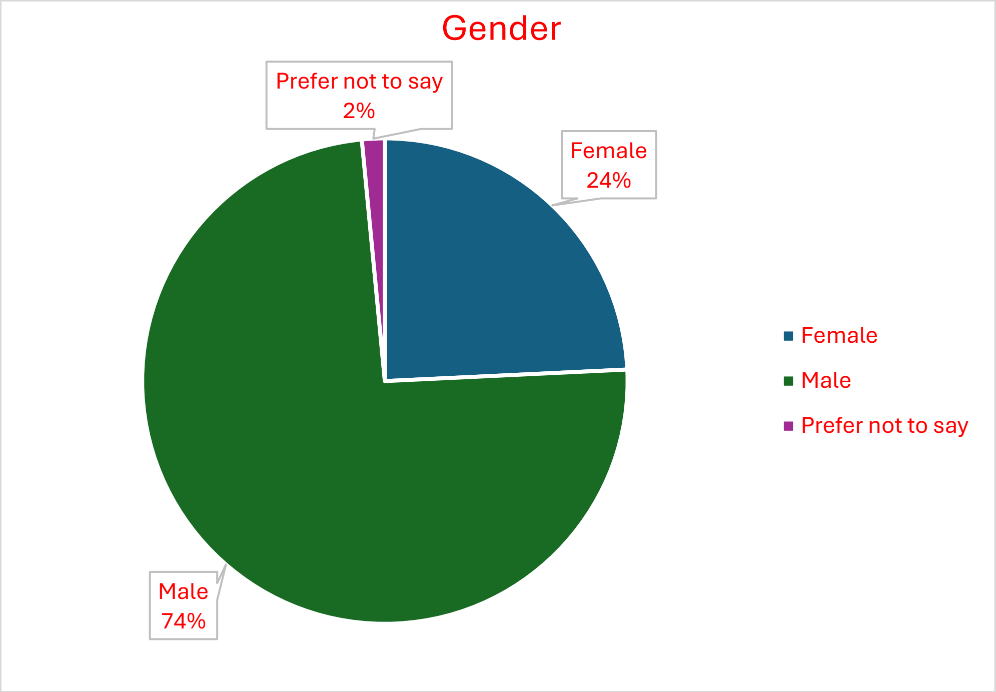


Figure 2 - Analysis of research participant's gender

Among the respondents there was a notable gender disparity, with male participants significantly constituting a large portion of the respondents. Of the 66 respondents, 74.24% (49) identified as male, 24.24 (16) identified as female. A small percentage, 1.52% (1) chose not to disclose information pertaining to their gender.

The 3:1 male-to-female ratio mirrors global trends in cybersecurity, where women represent only 25% of the workforce (World Bank, 2023). In Zimbabwe, this imbalance may stem from systemic barriers such as limited access to STEM education for women or cultural biases in IT hiring practices (Chikomba et al., 2023).

Implications for the Study:

1. **Bias Risk**: Male-dominated responses may overlook gender-specific challenges (e.g., women's access to cybersecurity training).
2. **Policy Gap**: The disparity underscores the need for initiatives like scholarships or mentorship programs to recruit women into cybersecurity roles, as diverse teams improve threat detection by 30%

4.2.1.2 Industry Sector:

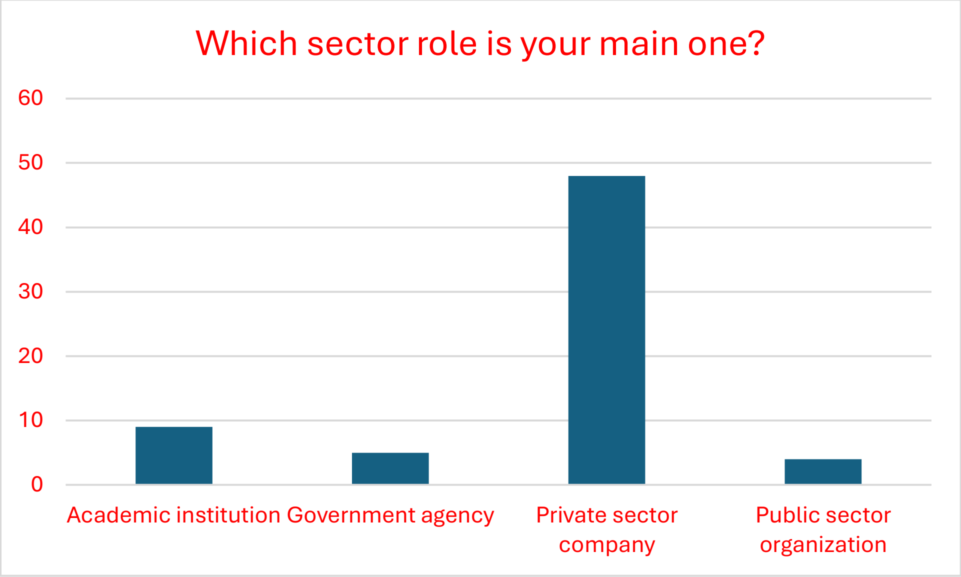


Figure 3-Analysis of research participants sectors of employment

The data indicates a significant representation of respondents from the private sector, with 48 out of 66 individuals employed in the private sector. This is followed by 13.64% (9) of the respondents working for academic institutions. Public sector organizations representatives constitute 6.06% (4) of the respondents, while government agencies take up 7.58% (5) of the remaining participants.

The distribution curve suggests the private sector plays a pivotal role in shaping the cybersecurity landscape in Zimbabwe. However, it is principal to acknowledge potential biases that may arise from this imbalance. The heavy representation of private-sector employees (72.73%) suggests findings may reflect corporate environments with better-resourced cybersecurity programs, potentially skewing perceptions of national readiness. Private-sector dominance may explain why 84.8% of respondents reported using firewalls/anti-malware (Section 4.2.3.2), a rate likely higher than national averages.

4.2.1.3 Cybersecurity level of experience:

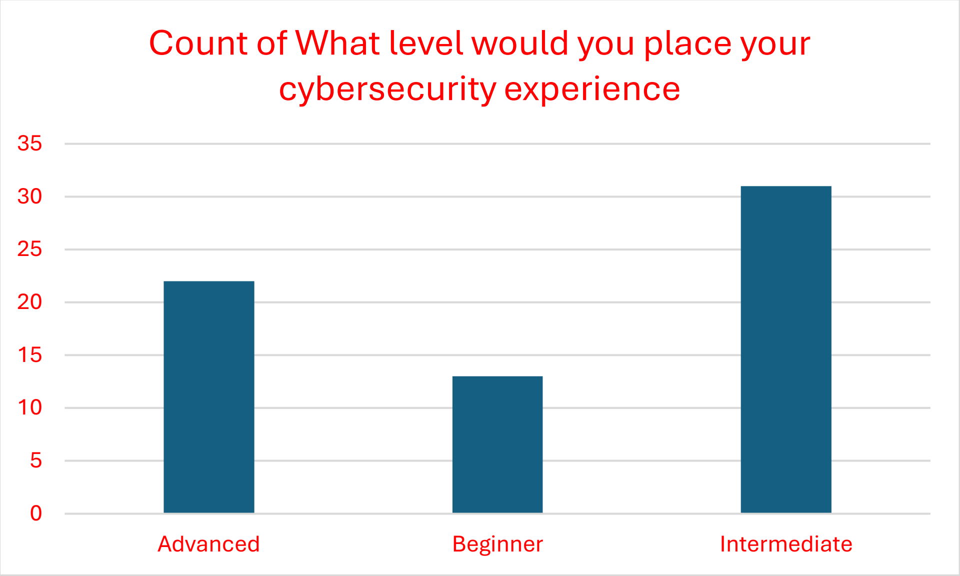


Figure 4-Analysis of research participants cybersecurity experience

From the respondents the majority categorized their cybersecurity experience as intermediate with 31 (46.97%) participants choosing this level. Indicating a cascade of experts with both fundamental knowledge as well as real world experience suggesting a moderate level of expertise. 22 (33.33%) of respondents regarded their cybersecurity experience as advanced, reflecting a higher level of proficiency as well as expertise in cybersecurity. On the lower end of the spectrum 13 (19.70%) of respondents described their cybersecurity experience to be of beginner, indicating limited exposure to cybersecurity concepts and practices.

These findings highlight the diversity of cybersecurity experience among the respondents. There is a strong representation of respondents with intermediate and advanced levels of expertise, however it is of vital importance the needs of beginners through targeted training and education programs are addressed to close the skills gap while enhancing the overall cybersecurity landscape in Zimbabwe.

4.2.2 Cybersecurity Awareness

4.2.2.1 Training and Education:

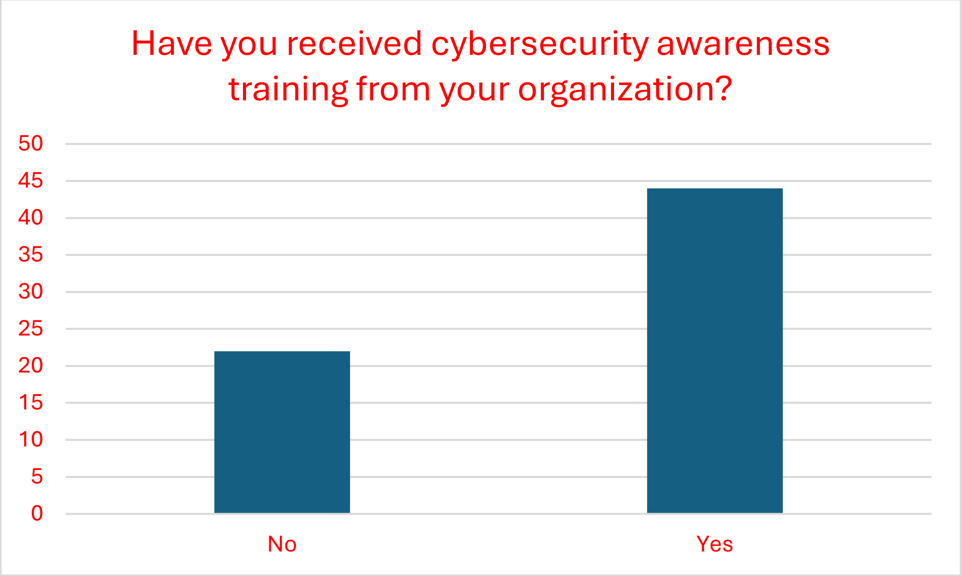


Figure 5-Graph on how many research participants have received cybersecurity training from work

To assess the level of cybersecurity awareness withing organizations, participants were asked whether they had received cybersecurity awareness training from their employer.
The results as shown in figure 6, indicate a majority of 44 respondents (66.7%) reported having undertaken cybersecurity awareness training, with 22 respondents (33.3%) having not received such training. Suggesting a proactive approach by a larger number of organizations towards cybersecurity training and education.

The findings suggest a majority of organizations are making strides in educating their employees on cybersecurity. A sizable proportion remains untrained, potentially highlighting the need for increased investment in cybersecurity awareness programs for organizations that have not yet implemented training initiatives.

These results underscore how crucial implementing comprehensive cybersecurity awareness programs across all levels of the organization. To strengthen the organizations security posture a high level of participation throughout the board is required, through equipping employees with the knowledge and skills required to identify and be capable to respond to potential risks and cyber threats effectively and efficiently.

To enhance cybersecurity awareness, organizations should consider undertaking regular training sessions, phishing simulations, tailored training as well as ensuring continuous learning. This places organizations in a position to empower their employees to play a vital role in maintaining and securing sensitive information and preventing cyberattacks.

4.2.2.2 Training Frequency**:**

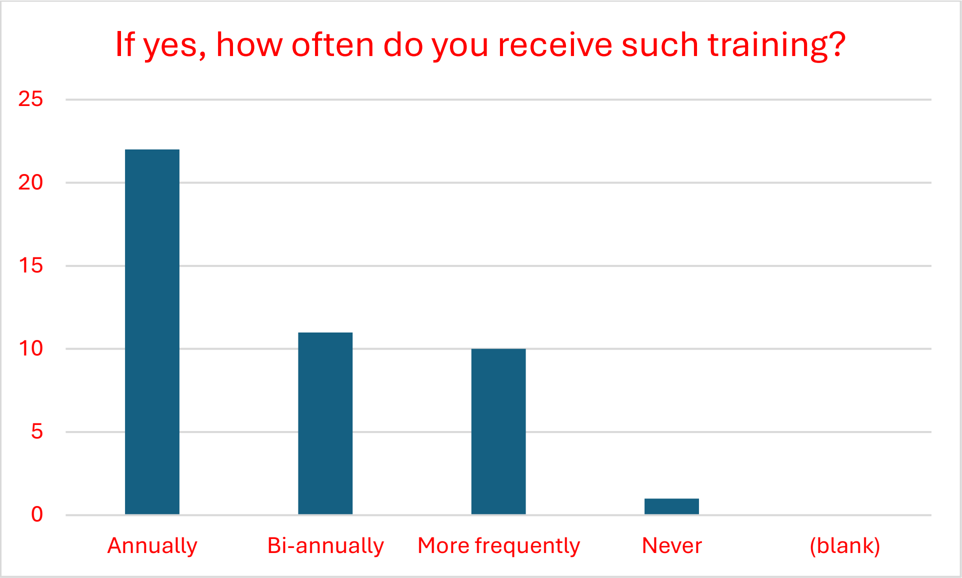


Figure 6-Graph on how frequent training is offered to participants

Following respondents who had received training participants were questioned on how often they underwent such sessions. The results illustrated in figure 7 reflect the responses. Among the results, 22 respondents (33.3%) indicated to receiving training on an annual basis, whereas 11 respondents (16.7%) indicated to having received training bi-annually. In addition to these 10 respondents (15.2%) receive training more frequently that bi-annually as well as annually, suggesting certain organizations are prioritizing continuous updates on cybersecurity practices.

Interestingly, 1 respondent indicted they did not receive further cybersecurity training following from the first time they undertook such training. This inconsistency indicates either a lack of regularized training routines or an oversight within their organizations administration.

The findings suggest annual cybersecurity training as a standard across the board in many organizations, with a smaller proportion moving toward more frequent sessions. Increasing the frequency or training sessions, especially paying special attention to those in roles that require frequent cybersecurity updates, may further strengthen the organizations defences to combat evolving cyber threats.

4.2.2.3 Impact of Awareness Initiatives:

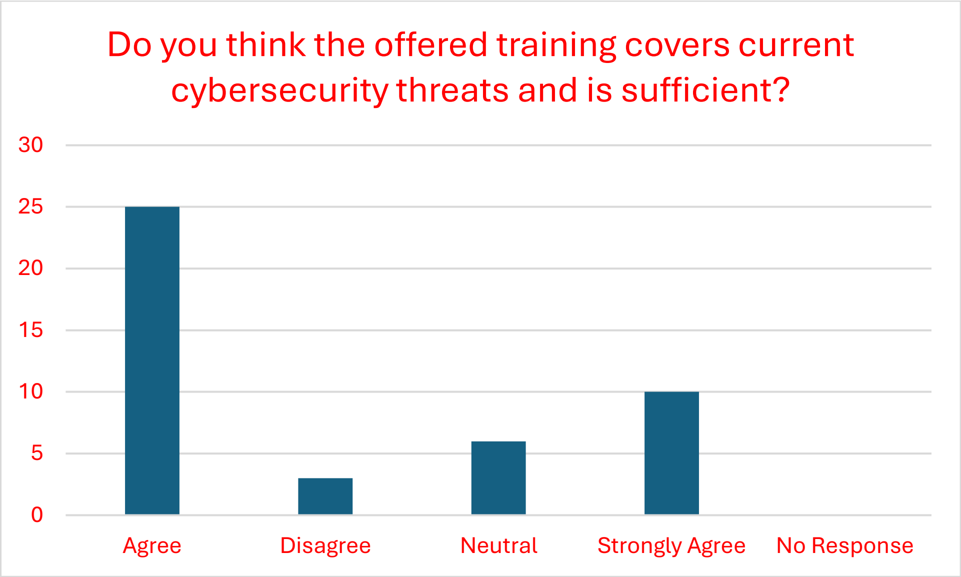


Figure 7-Graph of how effective respondents feel training is

Participants were asked if they believed the offered training covered current cybersecurity threats and if it was sufficient to their needs, this was as to evaluate the perceived effectiveness of cybersecurity training. Shown in figure 8, 25 respondents (56.8%) agreed that the training was sufficient, further to those 10 respondents (22.7%) strongly agreed, showing a positive view within over half of the participants.

On the other hand, minority expressed disagreement with the training's sufficiency, with 3 respondents (6.8%) stating a concerning inadequacy of the training, suggesting a potential gap in the effectiveness of current training programs. 6 respondents (13.6%) remained neutral, indicating mixed views or hesitancy regarding the applicability and depth of the training offered. While some portions of the training may have been effective, areas for improvement may still be made.

The distribution suggests that, while a large number of employees view the training as adequate, improvement is still possible in certain areas. Remaining up to date with the ever-evolving cyber threats is crucial when updating training content. Targeting and addressing the concerns of the neutral along with the dissatisfied creates an opportunity to further enhance the overall cybersecurity standing within organizations.

4.2.3 Organizational Culture

4.2.3.1 Perception of Cybersecurity Importance:

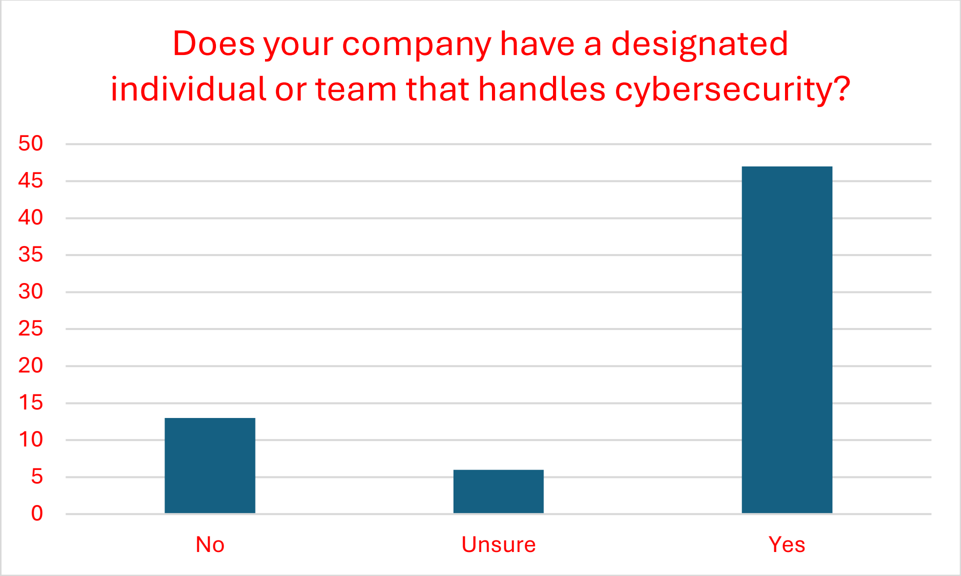


Figure 8-Graph showing if there is a cybersecurity response team at respondent organizations

Participants were questioned on whether or not their organizations had the presence of an individual or team dedicated to cybersecurity. Figure 9, illustrates 47 respondents (71.2%) confirming the presence of such a system within their organization, this indicates a vast majority of organizations formally employing cybersecurity management.

13 respondents (19.7%) indicated the absence of a cybersecurity team, hinting at a gap in organizational preparedness for cyber threats. While 6 respondents (9.1%) showed uncertainty at the presence of such a structure, suggesting a breakdown within some organizations about cybersecurity roles and responsibilities.

The presence of designated cybersecurity roles is a crucial aspect of an organization's overall cybersecurity frame. This team or individual ensures accountability as well as a well-versed system to address cybersecurity risks.

The responses pointing to a weak or lack of such roles highlights risk and potential vulnerabilities in cybersecurity infrastructure, these emphasize how crucial it is to communicate openly about cybersecurity jobs within organizations.

4.2.3.2 Leadership and Support for Cybersecurity:

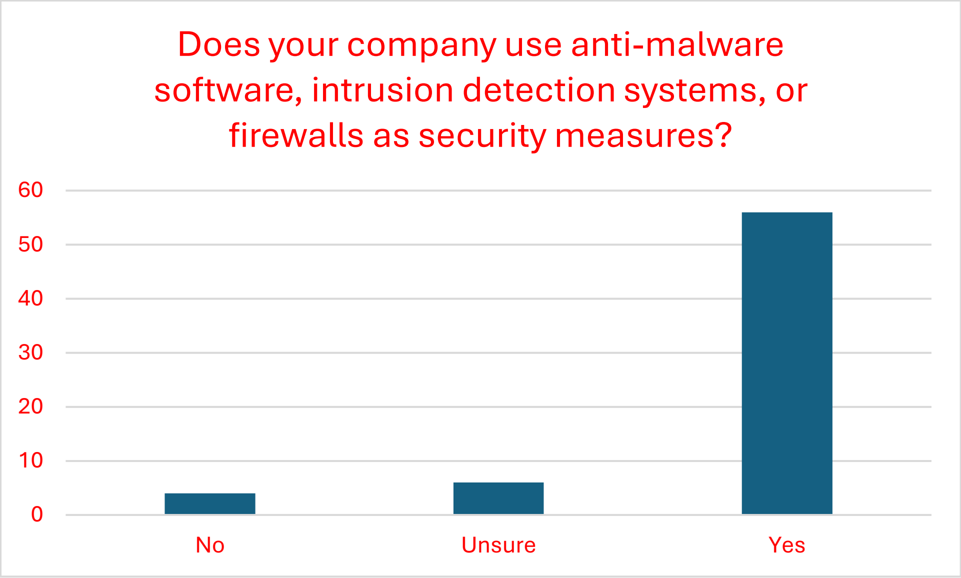


Figure 9-Graph of respondent's organizations security measures in place

Security Measure	**Zimbabwe**	**South Africa**	**Kenya**
Firewalls/Anti-malware	84.8%	98%	92%
Mobile Device Encryption	48.5%	85%	78%
Bi-Annual Cybersecurity Training	22.7%	62%	45%

Table 3- Security Tool Adoption vs. Regional Peers ITU Global Cybersecurity Index (2023)

An assessment of the implementation of technical of technical security measures within organizations was undertaken, with participants being questioned on whether their organizations utilized anti-malware software, intrusion detection systems or firewalls. These being base tools of a strong cybersecurity defence, that assist as well as deter unauthorized access along with malicious activities.

Figure 10, reveals a majority-56 respondents (84.8%) confirmed the utilization of these security measures within their organizations. The suggestion from this high adoption rate is that many organizations acknowledge the importance of protective technology in they cybersecurity implementation.

However, 4 respondents (6.1%) confirmed their organizations have not undertaken such measures, at the same time 6 respondents (9.1%) were uncertain of the presence of these tools. These subgroups indicate a risk to organizations being prone to cyber-attacks, the uncertainty indicated by some respondents reflects a gap in employee knowledge concerning their organizations security frame highlighting the importance of more transparent communication channels concerning cybersecurity.

The widespread use of these tools among majority of respondents organizations suggests a positive trend in basic cybersecurity defence. The earnest still remains to address gaps in both the adoption and awareness to ensure all employees understand the framework of the organization's cybersecurity.

4.2.3.3 Employee Practices and Attitudes:

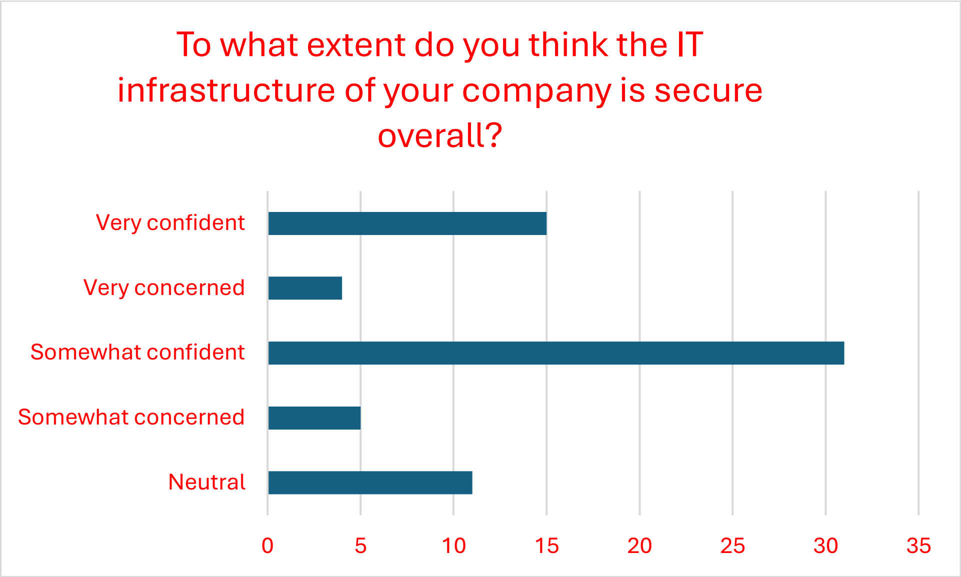


Figure 10-Graph showing extent to which participants feel their organizations feel their infrastructure is secure

Respondents were asked to score their degree of confidence in the overall security of their organizations IT infrastructure. Figure 11, illustrates a general positive outlook with majority, 31 respondents (47.0%) reporting feeling "somewhat confident' in their organizations overall IT security. Following those 15 respondents (22.7%) reported being "very confident."

A minority of participants indicate their organizations stance on the topic conveyed concern. 5 respondents (7.6%) reported they viewed their organizations were "somewhat concerned." Additionally, 4 respondents (6.1%) indicated their organizations seemed "very concerned." However, 11 respondents (16.7%) remained neutral, expressing neither concern nor confidence.

These findings suggest majority of employees are relatively secure with their organizations IT infrastructure, while a subset carries concerns. This discord may translate contrast in experiences or stages of awareness regarding security measures. Organizations stand to improve their security practices by paying attention to the areas of concern.

4.2.4 Existence of Explicit Guidelines and Protocols

In this section, participants were questioned on whether or not their organizations had explicit guidelines as well as protocols in place for various cybersecurity aspects, namely: management of passwords, control and access of data, incident reporting and security of mobile devices. The aim of this is aimed to assess the extent to which organizations are aiming to formalize cybersecurity practices to address vulnerabilities in security ensuring consistency in compliance.

Respondents had the selection of “yes”, “no” or “unsure” for each category. The data collected from this section provides an insight on organizational preparedness as well as employee awareness of security policies essential for mitigating cyber risks.

4.2.4.1 Password Management Guidelines:

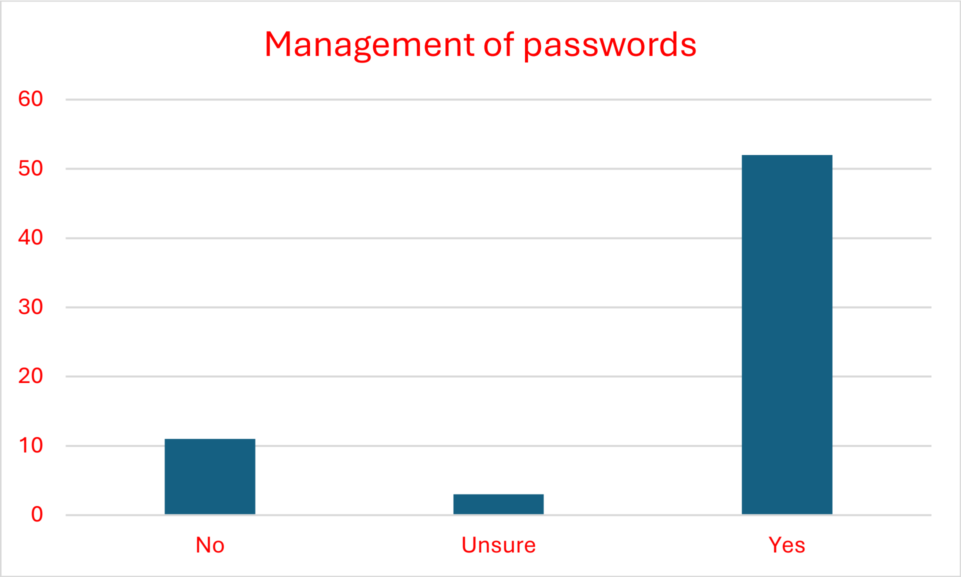


Figure 11-Graph showing guidelines and protocols on management of passwords

Out of the 66 participants, assessing whether organizations have explicit guidelines and protocols for the management of passwords. 52 (78.8%) indicated their organizations had established guidelines for password management. 11 (16.7%) indicated their organizations do not have such protocols in place. 3 (4.5%) stated they were unsure of the existence of password management policies.

According to the findings, a sizable majority of organizations recognize the importance of password management and have these guidelines implemented. However, the presence of those without protocols and those who are uncertain suggest the existence of gaps in either policy adoption or employee awareness.

Password management remains a keystone of cybersecurity, frailty in this area leaves a cybersecurity system vulnerable to infiltration. The finding points to a need for organizations to establish robust password management guidelines as well as ensure communication and enforcement across all levels of staff.

4.2.4.2 Control and Access of Data Policies:

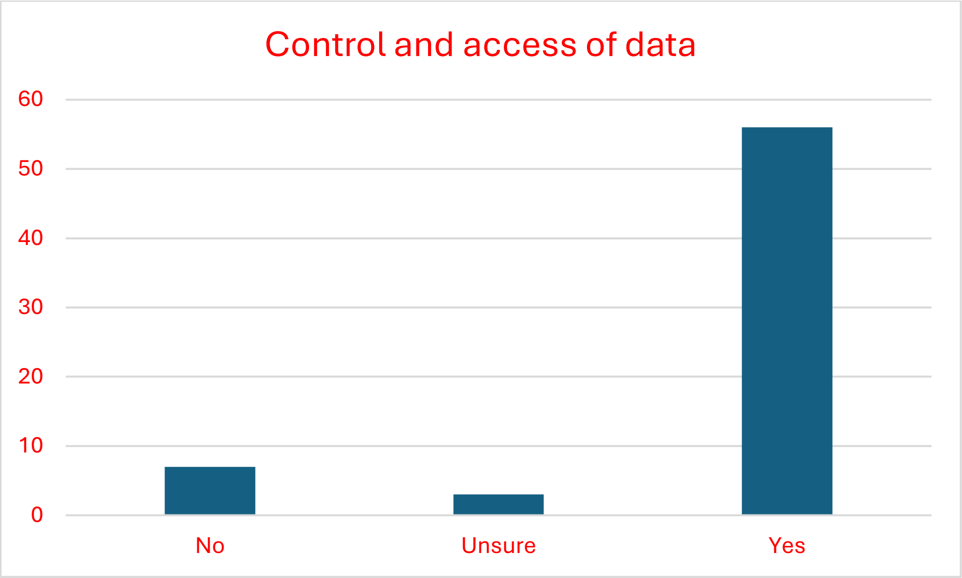


Figure 12-Graph showing guidelines and protocols on control and access of data

For control and access of data, 56 (84.8%) of respondents stated their organizations have clear guidelines and protocols in place. 7 (10.6%) stated their organizations lack these protocols. 3 (4.5%) of the respondents indicated uncertainty about the existence of these measures.

These findings indicate most organizations place a high priority on the protection of data access, via defined protocols. However possible weaknesses are highlighted by the missing protocols for the 10.6% along with the unsure 4.5% of respondents. For the protection of sensitive data and reduction of the likelihood of data breaches, it is crucial to ensure data access is strictly regulated and observed.

Organizations should ensure formal implementation of control and access to data, through employee training organizations stand to decrease illegal access and enhance overall data security.

4.2.4.3 Incident Reporting Mechanisms

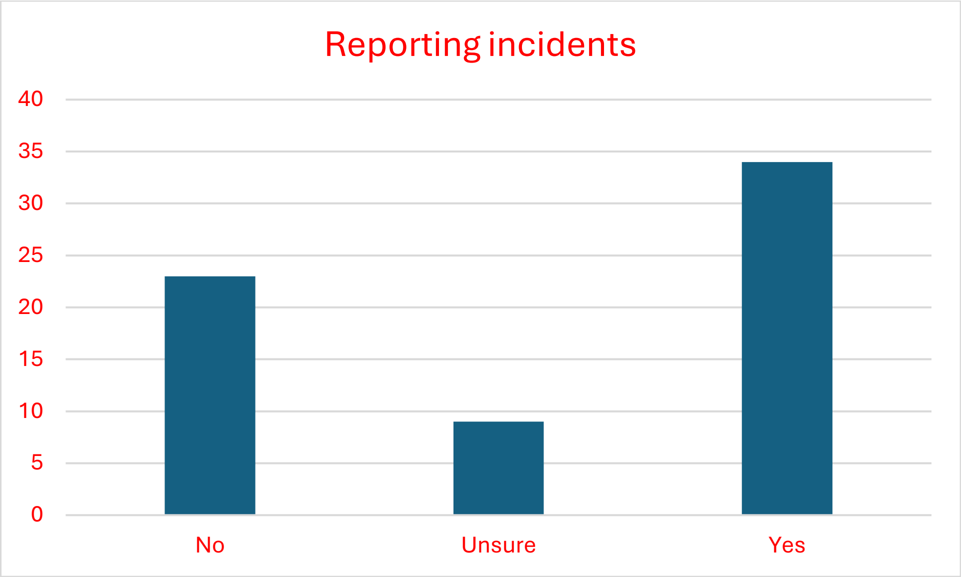


Figure 13-Graph showing guidelines and protocols on reporting incidents

Participants responded on the presence of guidelines and protocols on reporting incidents. 34 (51.5%) confirmed the presence of these protocols in their organizations. 23 (34.8%) indicated these protocols were not present in their organizations. 9 (13.6%) respondents were unsure about the existence of these guidelines.

Just over half of the respondents indicated that the reporting protocols existed withing their organizations. However, the remaining 48.5% who stated they either lack such protocols or are unaware of them, expose a critical gap. Reporting incidents promptly is crucial for security threats identification and mitigation in real time.

Organizations are encouraged to establish and implement clear incident response protocols which include and are not limited to: Reporting procedures, Investigation processes and communication plans. Organizations without these measures should look into establishing comprehensive incident reporting frameworks and effectively communicate these to all employees. This will enhance the reaction time to threats as well as harbour a proactive cybersecurity culture. Implementing these guidelines can significantly enhance the security posture of organizations.

4.2.4.4 Mobile Devices Security Measures

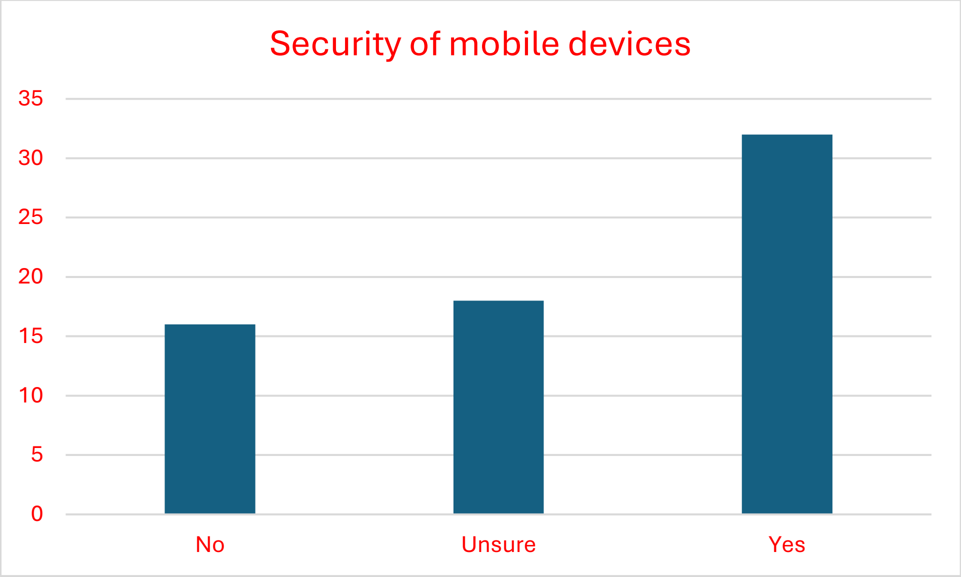


Figure 14-Graph showing guidelines and protocols on security of mobile devices

Respondents were evaluated on whether or not they had explicit guidelines for securing mobile devices. 32 (48.5%) indicated their organizations have such protocols in place. 16 (24.2%) stated that no such protocols exist in their organizations. 18 (27.3%) were unsure about the existence of mobile device security protocols.

These findings suggest a significant divide in awareness and implementation of mobile device security measures. Mobile devices are rapidly becoming more and more utilized for work purposes, such as accessing emails, company networks and sensitive data, creating a common entry point for cybersecurity threats. The organizations with lack of such protocols as well as limited employee awareness risk exposing sensitive data to vulnerabilities.

To protect mobile devices from cyber threats, organizations should look to implementing: remote wipe capabilities, regular software updates as well as data encryption. Awareness should also be conducted to ensure all employees remain informed about policies and the importance of securing mobile devices. The increasing use of mobile devices makes them an integral part of an organizations IT ecosystem. This also raises the possibility of them being a target area for cybercrimes.

4.3 Additional Comments

4.3.1 Key Suggestions for Strengthening Cybersecurity

The 66 respondents to the study were asked what steps governments as well as public institutions could implement to strengthen their cybersecurity framework. The following consolidates recommendations from the research participants, the aim is to provide actionable insights that can contribute to building a robust and adaptive cybersecurity ecosystem.

4.3.2 Recurring Themes in Respondents Feedback

The suggested responses were grouped into six primary themes, which highlight the crucial and critical areas for improvement as well as focus:

1. Training and Awareness

   Mentioned by over 50% of respondents these were the most frequently suggested solutions. Recommendations included but were not limited cybersecurity training programs through regular and thorough training for employees, students and the general public. Mandatory training regiments were suggested for workers to enhance their cybersecurity knowledge utilizing live demonstrations and workshops for practical learning.

Respondents pointed to awareness campaigns being utilized to educate citizens about cybersecurity safe practices and risks. Emphasis being placed on the risks of not having robust cybersecurity systems through public relation initiatives.

2. Development of Policies and Legislation

   Approximately 30% of respondents suggested stronger policies and legislation, with emphasis pointed toward the need for a comprehensive legal framework. Respondents suggested the development of a well-defined strategy to address cybersecurity broadly. Responses also included the enactment of stricter, clearer laws that are more adaptable to evolving threats, the introduction of mandatory IT security regulations as well would assist compliance across sectors. Additionally, respondents suggested the creation or strengthening of explicit protocols and standards for organizations to follow, particularly in areas such as data management and incident reporting.

3. Investment in infrastructure and technology

   20% of the respondents mentioned the investment in IT infrastructure and advanced technologies. Key areas were: modernizing infrastructure by the upgrading of outdated IT systems ensuring they are equipped to undertake current along with emerging threats. The investment in cutting edge cybersecurity tools namely, intrusion detection systems, firewalls and encryption mechanisms.

Furthermore, regular audits to identify vulnerabilities while assessing the readiness of systems

4. Collaboration and Expertise

   15% of respondents highlighted collaboration, public-private partnerships, public sectors leveraging private sector expertise along with technology to bolster initiatives in cybersecurity for the public sector. Respondents suggested organizations in Zimbabwe used global best practices through studying successful cybersecurity infrastructures in other countries to emulate their best practices.

5. Enforcement and Regulation

   Approximately 10% of respondents emphasized the vital role of accountability and enforcement, specific suggestions included: strict enforcement of laws, putting in place penalties for cybersecurity breaches to dissuade malicious activities. Furthermore, respondents highlight the need for conduction of regular system audits to regulate organizations adhere to cybersecurity regulations.

6. Other Suggestions

   A few additional suggestions highlighted encouraging innovation fostering an interest in research and development delving deeper into understanding cybersecurity technologies. Additionally, encouragement of investment into cybersecurity should be driven by implementing policies that are business friendly.

4.4 Discussion of Results

4.4.1 Key Findings

The analysis of the research results brought to light several critical insights that delve into Zimbabwe’s cybersecurity readiness and infrastructure. In addition to the structured survey questions, respondents had the opportunity to share comments or suggestions regarding Zimbabwe’s cybersecurity landscape.

This open-ended question afforded participants the opportunity to express unique perspectives, challenges along with insights. A significant portion (58%) of respondents indicated they had no additional input, while 42% of respondents provided valuable insights. Sub-categorized into the recurring themes below:

1. Training, awareness and education:

   Respondents emphasized the vital role training and awareness campaigns play in equipping individuals and organizations with key cybersecurity knowledge. Respondents made the following comments on how training and awareness can assist Zimbabwe’s Cybersecurity infrastructure:

   - “Improved awareness strategies.”
   - “Training and public awareness campaigns.”

2. Modernization and Infrastructure investment

   Respondents further highlighted the outdated nature of Zimbabwe’s IT and cybersecurity infrastructure, respondents had this to say:

   - “The lack of adequate infrastructure in Zimbabwe, the lack of awareness of citizens, and the economic challenges have compounded to the point that cybersecurity in the nation is sorely lacking for the current age.”
   - “Update infrastructure.”
   - “We need to move with the times.”

3. Global Benchmarking and Collaboration

   A few respondents had suggestions towards Zimbabwe learning from global best practices and engaging international expertise, respondents made the following comments:

   - "Zimbabwe needs to update its cybersecurity systems to the current ones being used in developed countries."
   - "Engage experts even from other countries to work on putting cybersecurity systems in place."

4. Industry specific concerns

   Some respondents highlighted the specific needs of industries such as financial institutions and telecom companies, one respondent had the following to say:

   - "Institutions that heavily rely on user databases, for instance, financial institutions and telecom companies, should have effective data governance frameworks."

5. Legal and Policy frameworks

   Respondents underscored the necessity of robust legal frameworks and policies for the regulation of cybersecurity behaviours, specifically respondents commented with:

   - "Emphasis should be placed on bolstering legal frameworks and policies that push for adoption of the most current up-to-date practices."
   - "Enact flexible and clear legislation for effective data governance, particularly in financial and telecom institutions."

6. Contextual Challenges

   Barries to improving cybersecurity were acknowledged by respondents, namely economic and leadership challenges, highlighted comments made by respondents included:

   - "It's hard to provide constructive views on cybersecurity when Zimbabwe's infrastructure (IT included) is in tatters."
   - "Poor governmental leadership and lack of infrastructure investment means cybersecurity remains a low priority unless connected to banking and remittances."

7. Miscellaneous Suggestions

   Respondents furthermore made comments emphasizing localized or unique views, these comments included:

   - "Needs homegrown solutions."
   - "Practitioners should form a professional industry body such as the Institute of Chartered Accountants to promote the profession."
   - "At what scale is investment into cybersecurity worth it? Small institutions may not have sensitive data to justify high costs."

While over half of the respondents made no further comments, this may suggest a lack of awareness or confidence in cybersecurity expertise. This demographic should be the focus of public awareness and training initiatives to increase participation in cybersecurity conversations.

However, the recurring issues raised by respondents pointed to the key focus areas for improvement being: Infrastructure modernization, training programs and global collaboration. Organizations in Zimbabwe according to respondents should strengthen their legal frameworks through ensuring clear, enforceable and adaptable cybersecurity laws. Localized solutions coming from respondents included investing in homegrown cybersecurity solutions addressing local challenges while leveraging global expertise.

4.4.2 Implications for Cybersecurity in Zimbabwe

The findings bring to light that although strides have been made in boosting awareness of cybersecurity as well as establishing protocols considerable gaps remain,

Organizational Resilience: From the responses regarding mobile device security and incident reporting there is an indication that many organizations are not prepared for sophisticated cyber threats. Less than half the respondents indicated a robust mobile device security protocol, raising alarm in an ever-evolving technological age.

With only 52% of respondents affirming the presence of incident reporting mechanisms, a significant risk may be faced by organizations as security breaches may go undetected and unresolved.

Workforce Preparedness: Employees are left exposed and unprepared to evolving threats due to the insufficient training's frequency, this in turn leaves organizations exposed to higher risks. With only 22% of respondents receiving training annually and 10% more frequently, suggests a lack of investment in workforce preparedness. Furthermore, there is an indication that existing programs are insufficiently tailored against emerging threats.

Zimbabwean organizations must prioritize more frequent, understandable cybersecurity training, taking into consideration realistic and emerging threat landscapes to strengthen employees as the first line of defence.

Cybersecurity is not yet ingrained within organizational culture, indicated by the lack of active engagement with employees. A cultural shift is required, to promote a culture of shared responsibility and accountability. This will further push for a more proactive cybersecurity readiness across all levels.

National Readiness: On a national level based off the findings, Zimbabwean cybersecurity infrastructure is weak compounded by economic and political challenges. These findings suggest a hinderance to the nation's ability to develop and enforce comprehensive cybersecurity strategies. Respondents repeatedly hinted to outdated infrastructure as a hinderance on cybersecurity effectiveness.

The government along with the private sector must collaborate to modernize Zimbabwe's IT infrastructure, placing a priority towards upgrades that align with international standards. Participants emphasized the need for dynamic legislation that remains head-to-head with global trends and advancements in technology. This must be accompanied by a comprehensive national cybersecurity strategy developed, with clear policies and stringent regulations. Allocating resources strategically for the technology sector, including trainings and policy implementation will help to combat the restraint placed on cybersecurity enhancement advancement.

The need for resource sharing was highlighted by respondents that brought to light an absence of robust collaboration among the government, private institutions and international stakeholders. Respondents highlighted the importance of emulating cybersecurity models from other nations, partaking in global forums to adopt best practices and align Zimbabwe’s cybersecurity strategy with global standards to address cross-border threats.

As a final point respondents pointed to a low level of public awareness among the general public, this leaves organizations as well as individuals alike susceptible to cyberattacks. Mimicking health initiatives, through the utilization of nationwide awareness campaigns to educate about basic cybersecurity practices must be adopted. In conclusion the implications of this study highlight that cybersecurity is merely not just a technological issue but a conglomerate requiring a harmonized course of action across all levels.

A comparison of the cybersecurity readiness of Zimbabwe with that of South Africa, Kenya, and Nigeria indicates major gaps. South Africa takes the lead in cyber defense thanks to its National Cybersecurity Strategy and AI-powered security systems. Kenya, the fintech leader, has enforced stronger data protection legislation to counter cyber fraud. Nigeria has instituted cybersecurity policies to tackle financial cybercrimes.

Zimbabwe is lagging due to outdated IT infrastructure, lax implementation of cybersecurity policy, and minimal public awareness. To bolster its cybersecurity situation, Zimbabwe should adopt a policy like Kenya's regulatory environment in conjunction with spending in AI-enabled security solutions like in South Africa

4.4.3 Limitations of Study

While the study offered insightful information, several limitations must be noted:

Sample Representation:

The research study focused on 66 participants; this size may not completely represent the range of organizations in Zimbabwe which are completely diverse.

Response Bias:

The term response bias, or response set, refers to a systematic deviation of the reported respondent values from the true values (Bogner and Landrock, 2016). Some respondents provided neutral or vague responses, hindering the depth of analysis for certain questions.

Self- Reported data:

Self-reported data cannot be independently verified and can contain several potential bias sources, such as selective memory, attribution, and exaggeration. These biases become apparent if they are incongruent with data from other sources. Brutus, et al. (2013). Participants may overestimate or underestimate their organizations cybersecurity awareness or practices. Whereas some respondents might have withheld crucial information about the practices of their organizations due to confidentiality concerns.

CHAPTER 5: CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This Chapter summarizes the key findings of the study, delves into their implications and furthermore offers recommendations for strengthening Zimbabwe's cybersecurity readiness and infrastructure. The aim of the study was to assess Zimbabwe's current posture on cybersecurity, pinpoint gaps and propose workable solutions.

These findings are supported by information from the literature review along with the analysis of data collected from 66 respondents from a various number of industries across Zimbabwe.

5.2 Discussion

Reiterating the discussion in chapter 4, the findings reveal that while Zimbabwe has made progress towards addressing cybersecurity challenges, there are still large gaps in infrastructure, policy execution and awareness.

Key Findings Discussed:

1. **Cybersecurity Awareness and Training**

   The majority of respondents, (66.7%) reported they had received cybersecurity awareness training, there was significant variation in the frequency and scope of these programs. Many respondents noted that training was too inadequate to handle contemporary threats.

Awareness initiatives along with frequent training were highlighted as crucial and necessary for bridging the gap in knowledge among employees and the public alike.

2. **Organizational Readiness**

   A commitment to cybersecurity measures was displayed, with 84.8% of respondents indicating their organizations utilization of basic security measures such as, firewalls and anti-malware tools. A majority of respondents (71.2%) also indicated this was the case with their organizations employing and implementing a cybersecurity workforce.

   Nonetheless, a presence of gaps was presented in mobile device security, with only 48.5% of respondents indicating their organizations had protocols in place. With incident reporting mechanisms being available in slightly over half (52%) of the respondents' organizations, an indication of vulnerabilities that need urgent attention was made apparent.

3. **National Infrastructure and Legislation**

   Citing outdated IT systems and insufficient investment in technology, respondents identified these as major barriers to cybersecurity awareness. The findings suggest Zimbabwe's legal framework to be inadequate to address emerging threats, prompting calls for strong, adaptive and enforceable cybersecurity regulations.

4. **Public Awareness and Collaboration**

A recurring theme contributing to the significant risk present in Zimbabwe was the limited awareness of cybersecurity issues. Respondents urged the need for public-private partnerships and international engagement to develop Zimbabwe's cybersecurity ecosystem.

5.3 Conclusions

Based on the results, the following conclusions can be drawn up:

1. **Insufficient Cybersecurity Awareness**

   Despite the efforts many organizations are taking to educate their employees, the overall level of awareness concerning cybersecurity remains meagre. This crevice in education and understanding renders organizations and individuals susceptible to an extensive range of cyber threats.

2. **Infrastructure Gaps Limit Readiness**

   The widespread utilization of outdated IT infrastructure and limited advocacy for advanced technology largely cripples Zimbabwe's ability to combat evolving threats in the evolving cyber space landscape.

3. **Policy and Legal Frameworks are Underdeveloped**

   Feeble cybersecurity legislation and poor enforcement mechanisms render it challenging to establish a comprehensive defence against cybercrime. These hinder multiple aspects across the nation's cybersecurity preparedness, stemming from current threats to ensure a sustainable protection against future risks.

4. **Collaboration and Innovation are Lacking**

   Zimbabwe is still developing and is yet to fully capitalize on public-private partnerships. Reiterating the claims of respondents, global-best practices are a fundamental keystone in addressing Zimbabwe's cybersecurity challenges.

5.4 Recommendations

Based off of the study's, results and conclusions, the following solutions are recommended to improve Zimbabwe's cybersecurity readiness and close identified gaps. These suggestions are intended for certain stakeholders, namely, organizations, governments, academic institutions and the general public, to guarantee a comprehensive and sustainable approach to improving cybersecurity infrastructure and awareness.

Recommendations for Organizations

Organizations are advised to adopt a proactive approach to cybersecurity by creating comprehensive policies that address key areas such as password management, mobile device security, incident reporting and data access restrictions. Following the implementation of these policies they must be regularly reviewed and updated to combat and stay up to date with emerging threats.

Furthermore, organizations must place a priority on the need for investment in technologies such as intrusion detection systems and AI powered tools, to protect their infrastructure and data effectively. Organizations must put in place mandatory, ongoing and specifically tailored training programs for their employees that assist in combatting cyber threats. Organizations must implement or strengthen existing cybersecurity defence forces, adopting a zero-trust security model, which places a limit on access levels based on the principle of least privilege.

Organizations, government and private alike, must get proactive in protecting their online assets and ensuring business continuity in spite of the evolving threats of cybercrime. One of the most effective ways is to have a Zero Trust Architecture (ZTA), which follows the philosophy of "never trust, always verify." It requires continuous authentication and authorization, thus access to sensitive systems and data is provided based on real-time verification and not implicit trust.

Some of the most important steps include deploying multi-factor authentication (MFA) to increase identity security, deploying encryption protocols to protect sensitive information, and constantly updating access controls based on employee roles and responsibilities to minimize insider threats.

Global technology leaders such as Google and Microsoft have been able to implement the Zero Trust model, which demonstrates its effectiveness in reducing attack surfaces and preventing unauthorized access. Through adopting these best practices, organizations in Zimbabwe have the potential to significantly enhance their cybersecurity position, reduce data breach vulnerability, and develop a strong digital foundation.

Recommendations for Policymakers and the Government

At national level this is the most pivotal role to play to combat cyberthreats and crimes. Finalizing and strictly implementing the National Cybersecurity Policy regularly should be a priority, with a standardized interval for amendments. This policy must go hand in hand with international standards while providing clear guidelines for compliance at all levels.

Additionally, establishing a National Cybersecurity Operations Centre could assist in bringing about a centralized mechanism for monitoring, detecting and acting upon threats. Modernization of critical infrastructure should be of top priority to policymakers particularly in sectors such as finance, telecommunications, healthcare and energy. Addressing issues such as data protection, ransomware and digital identity management through dynamic legislations is another step to be taken in the legal framework, ensuring strict enforcement. Creating a safer and more predictable digital landscape.

Recommendations for Academia and Research Institutions

Aforementioned, no level is exempt, these institutions have a crucial role to play in improving the nations cybersecurity posture. Cybersecurity should be meshed into educational curricula at all levels, with programs tailored to coincide with global industry standards. Universities can also contribute by investing in research into Zimbabwean-specific cybersecurity obstacles, delving into the unique needs of rural and urban areas alike.

Researchers, students and professionals could collaborate to spearhead cutting edge projects, within Cybersecurity centres of excellence. These centres could host hackathons and workshops to take strides in the development of a stronger cybersecurity community. Academic institutions play a pivotal role in cultivating the next generation of cybersecurity professionals and advancing research in the field. To strengthen Zimbabwe’s cybersecurity ecosystem, universities should introduce specialized degree programs and industry-recognized certifications tailored to current and emerging cyber threats. This can be achieved through strategic partnerships with international institutions to develop accredited cybersecurity curricula that align with global best practices.

In addition, institutions of higher education should include cybersecurity modules in today's IT and computer science course curricula so that all graduates have fundamental cyber defence skills. Offering professional certifications such as Certified Information Systems Security Professional (CISSP) and Certified Ethical Hacker (CEH) would enhance job prospects and hands-on application know-how in the field of cybersecurity.

One of the models that has worked and could be replicated in Zimbabwean universities is the University of Cape Town Master's program in Information Security, which gives students higher level skills in cryptography, network security, and risk management. In adopting such courses, universities have an important role to play in closing the cyber skills gap as well as instilling a research-oriented culture of national cyber resilience.

Recommendations for the General Public

Through public awareness campaigns, the general public must engage in the broader effort to improve cybersecurity. Focus must be aimed towards educating citizens about common cyber risks and best practices, namely recognizing phishing attempts and securing personal devices. Vulnerable populations should be targeted and educated on digital literacy, to ensure all segments of society are equipped to swiftly navigate the digital age safely. Individuals must learn and understand responsible digital practices to enhance individual cybersecurity resilience, such as using strong passwords, enabling multi-factor authentication and regularly updating software.

For more awareness Zimbabwe should use social media, radio, and television to educate citizens on common cyber threats like phishing and ransomware.
Having easy-to-understand materials written in local languages such as Shona and Ndebele will enable them to reach a greater number of people and ensure understanding across diverse groups.
The involvement of NGOs and community leaders is central in spreading cybersecurity consciousness in rural communities where digital knowledge may be poor. For example, Kenya's "Be the Shield" initiative has been able to educate citizens regarding best practices in cybersecurity, demonstrating the effectiveness of nationwide awareness drives.

Actionable Cybersecurity Roadmap for Zimbabwe

For an improved Zimbabwe cyber environment, a structured plan must be initiated:

Short-term (1-2 years):

- Make it a requirement to deliver cybersecurity training for government workers and private sector workers.
- Implement robust enforcement of the Cyber and Data Protection Act (2021).
- Develop an incident response plan for handling cybersecurity events.

Mid-term (3-5 years):

- Invest in threat detection response mechanisms powered by artificial intelligence.
- Introduce a National Cybersecurity Operations Centre to monitor and respond to cyber threats in real time.

- Launch a cybersecurity awareness campaign targeting businesses and individuals.

Long-term (5+ years):

- Upgrade national IT infrastructure to align with global cybersecurity standards.
- Establish a cybersecurity research and development hub in collaboration with universities and the private sector.
- Foster international partnerships to exchange best practices and improve Zimbabwe's cybersecurity resilience.

Conclusion

By embracing these recommendations, Zimbabwe can take strides in positioning itself as a regional leader in cybersecurity. The growing digital age requires, strong institutions, businesses and citizens. The stakeholders are key to a nation achieving its vision and assuring a safe and secure digital future.

List of References

Africa Cyber-Security Report. (2024). https://www.linkedin.com/posts/interpol_out-now-the-2024-african-cyberthreat-assessment-activity-7192188390212083712-Tnsi/

African Union. (2024). Continental cybersecurity strategy: Implementation in Southern Africa. AU Press. https://au.int/sites/default/files/documents/44004-doc-EN-_Continental_AI_Strategy_July_2024.pdf

Barbian, B. (2015). *Research design and methodology in administration and law.* LexisNexis South Africa.

Braun, V., & Clarke, V. (2022). Thematic analysis: A practical guide (2nd ed.). Sage.

Brutus, S., Aguinis, H., & Wassmer, U. (2013). Self-reported limitations and future directions in scholarly reports: Analysis and recommendations. *Journal of Management, 39*(1), 48-75.

Chen, L. (2003). Examining technology acceptance by integrating social cognitive theory with user characteristics. *Journal of the Association for Information Systems, 4*(1), 11. https://journals.sagepub.com/doi/full/10.1177/1460458219879337

Chikomba et al. (2020). Management of digital records in selected financial services parastatals in Zimbabwe. https://www.deepdyve.com/lp/sage/management-of-digital-records-in-selected-financial-services-VB5nLJ0UJH?key=sage

Chikomba, A., Ndlovu, T., & Moyo, L. (2023). Cybersecurity challenges in Zimbabwe's financial sector. Zimbabwe Journal of Technology, 12(2), 45-67. https://f1000research.com/articles/12-1251

Creswell, J. W., & Creswell, J. D. (2023). Research design: Qualitative, quantitative, and mixed methods approaches (6th ed.). Sage.

Darktrace. (2023). *AI in African cybersecurity* (White Paper No. DT-2023-04, pp. 1-15). https://www.darktrace.com

Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. *Journal of Nursing Education, 48*(6), 105-112. https://pubmed.ncbi.nlm.nih.gov/18352969/

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. American Journal of Theoretical and Applied Statistics, 5(1), 1–4. https://doi.org/10.11648/j.ajtas.20160501.11

Fungai, J. (2024). Government steps up efforts in cybersecurity awareness. Retrieved from https://www.zbcnews.co.zw/government-steps-up-efforts-in-cyber-security-awareness/

Herjavec. (2019). *2019 official annual cybercrime report.* *https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf*

Mukiibi H. (2019) Cyber security in Africa: The boring technology story that matters. Crossroads. https://dl.acm.org/doi/abs/10.1145/3368077

Weforum. (2022) Global Cybersecurity Outlook. https://www.seekingfire.com/business/world-economic-forum-global-cybersecurity-outlook-2022-what-you-need-to-know/#:~:text=%E2%80%9CThe%20rise%20of%20supply%20chain,or%20C%2Dsuite%20level.%E2%80%9D

Information Security Institute (ISI). (2014). *Critical terminology foundations 2: Russia-U.S. bilateral on cybersecurity.* East West Institute. Retrieved from https://www.files.ethz.ch/isn/178418/terminology2.pdf

International Organization for Standardization. (2022). ISO/IEC 27001: Information security management systems.

International Telecommunications Union (ITU). (2008). *X.1205 Overview of cybersecurity. Series X: Data Networks, Open System Communications and Security – Telecommunication Security.* Retrieved from https://www.itu.int/rec/T-REC-X.1205-200804-I

James, M. (2017). National cybersecurity strategies in developing countries: A case study of Kenya. *Journal of Information Warfare Theory and Practice, 5*(2), 117-132.

Kabata, C. (2018, July 18). The state of cybersecurity in Zimbabwe. *The Zimbabwean.*

Machaka, L. (2021, June 23). Zimbabwe's public sector ill-equipped to deal with cyber threats. *The Herald.*

Madondo, T. (2017, August 29). Zimbabwe's lack of cybersecurity leaves it prone to cybercrime. *TechZim. https://www.techzim.co.zw/2017/11/underestimated-cybercrime-zimbabwe-time-woke-now/*

Majome, T. (2017, August 21). Zimbabwe's Cybercrime Bill: A threat to freedom of expression. *Open Dialogue.*

Martins, L. L., Oliveira, D. S., & Pappas, M. R. (2021). A systematic literature review of cybersecurity awareness and training programs in government institutions. *Journal of Information Systems Education, 32*(3), 189-210.

Merriam-Webster Dictionary (MW). (2020). Cybersecurity. Retrieved from https://www.merriam-webster.com/dictionary/cybersecurity

Microsoft. (2022). *Zero Trust adoption report* [Industry report]. https://www.microsoft.com/security/blog/zero-trust-adoption-report/

National Institute of Standards and Technology. (2021). Cybersecurity framework version 2.0. U.S. Department of Commerce. https://www.nist.gov/cyberframework

Njanjamangezi, T. (2014, August 28). Over 90% of Zimbabwean organisations face cybersecurity threats. *TechZim. https://www.techzim.co.zw/2024/08/zim-is-3rd-most-attacked-country-in-world-cause-cybersecurity-is-joke-to-us/*

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. Administration and Policy in Mental Health, 42(5), 533–544. https://doi.org/10.1007/s10488-013-0528-y

Parasuraman, A. (2000). Technology readiness index (TRI): An overview. *Journal of Industrial Management, 11*(2), 308-320.

Peter, A. S. (2017). Cyber resilience preparedness of Africa's top-12 emerging economies. *International Journal of Critical Infrastructure Protection, 17,* 49-59. https://ideas.repec.org/a/eee/ijocip/v17y2017icp49-59.html

Postal and Telecommunications Regulatory Authority of Zimbabwe. (2023). National cybersecurity report: Threat landscape in Zimbabwe. https://f1000research.com/articles/12-1251

PwC. (2014). *Global State of Information Security Survey 2014. https://www.pwc.com/na/en/assets/pdf/global-state-of-information-security-survey-2014-key-findings-report.pdf*

PwC East Africa. (2022). *Kenya's data protection impact* [Consulting report]. Nairobi: PwC. https://www.pwc.com/ke/en/publications.html

Reserve Bank of Zimbabwe (RBZ). (2015). *Thematic report on financial inclusion.*

Saunders, M., Lewis, P., & Thornhill, A. (2019). Research methods for business students (7th ed.). Pearson.

Schreier, M. (2018). Qualitative content analysis in practice. Sage.

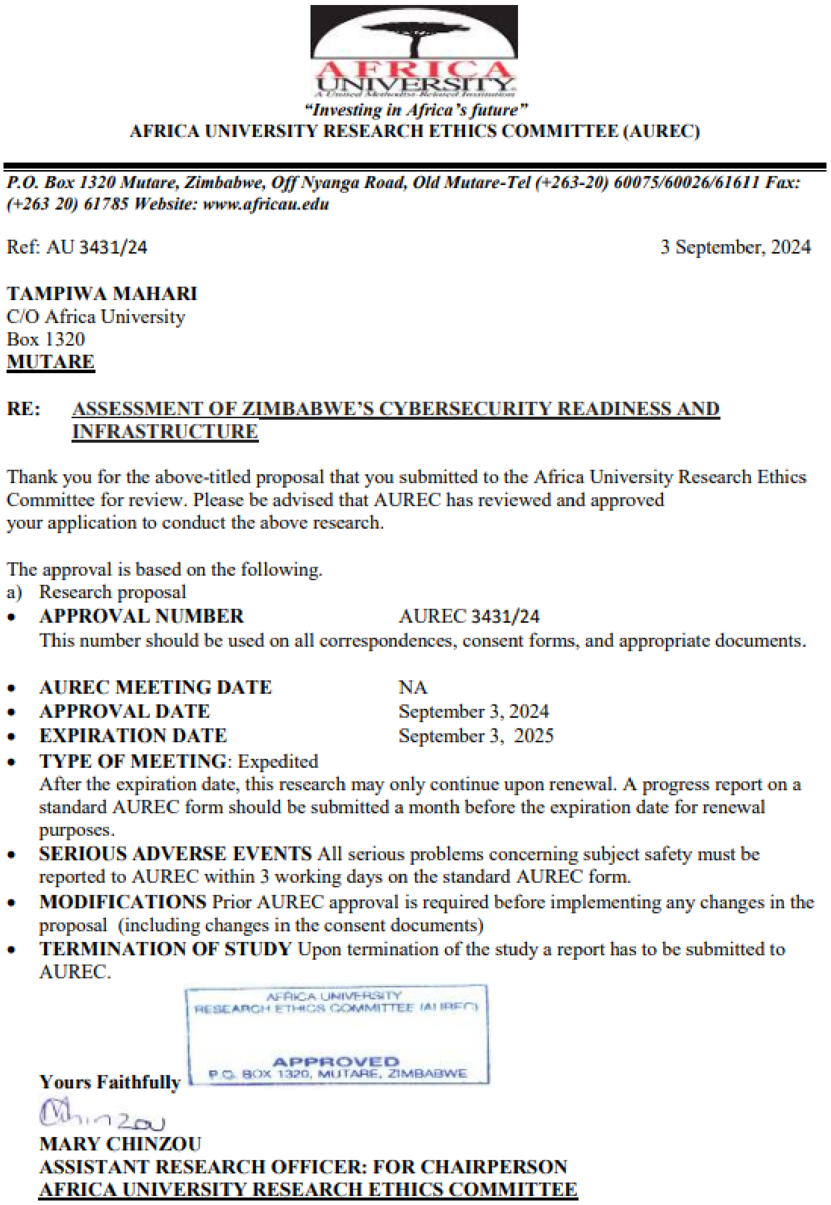
Surveys Kathrin Bogner & Uta Landrock (2016). Response biases in standardised surveys.

World Bank. (2023). *Digital infrastructure investment in developing nations* [Policy report]. Washington, DC: World Bank Group. https://www.worldbank.org/en/topic/digitaldevelopment

Zimbabwe Democrats Institute (ZDI). (2018, August 21). ZDI urges caution on Cybercrime Bill.

Zimbabwe Cyber and Data Protection Act. (2021). *Government Gazette, 99*(12), 1-45 [Legislation]. Harare: Government Printers.

Appendix 1 : AUREC Approval Letter



"Investing in Africa's future"

AFRICA UNIVERSITY RESEARCH ETHICS COMMITTEE (AUREC)

P.O. Box 1320 Mutare, Zimbabwe, Off Nyanga Road, Old Mutare-Tel (+263-20) 60075/60026/61611 Fax: (+263 20) 61785 Website: www.africau.edu

Ref: AU 3431/24 3 September, 2024

TAMPIWA MAHARI
C/O Africa University
Box 1320
MUTARE

RE: ASSESSMENT OF ZIMBABWE'S CYBERSECURITY READINESS AND INFRASTRUCTURE

Thank you for the above-titled proposal that you submitted to the Africa University Research Ethics Committee for review. Please be advised that AUREC has reviewed and approved your application to conduct the above research.

The approval is based on the following.

a) Research proposal

- **APPROVAL NUMBER** AUREC 3431/24
  This number should be used on all correspondences, consent forms, and appropriate documents.

- **AUREC MEETING DATE** NA
- **APPROVAL DATE** September 3, 2024
- **EXPIRATION DATE** September 3, 2025
- **TYPE OF MEETING**: Expedited
  After the expiration date, this research may only continue upon renewal. A progress report on a standard AUREC form should be submitted a month before the expiration date for renewal purposes.
- **SERIOUS ADVERSE EVENTS** All serious problems concerning subject safety must be reported to AUREC within 3 working days on the standard AUREC form.
- **MODIFICATIONS** Prior AUREC approval is required before implementing any changes in the proposal (including changes in the consent documents)
- **TERMINATION OF STUDY** Upon termination of the study a report has to be submitted to AUREC.

AFRICA UNIVERSITY
RESEARCH ETHICS COMMITTEE (AUREC)
APPROVED
P.O. BOX 1320, MUTARE, ZIMBABWE

Yours Faithfully

Chinzou

MARY CHINZOU
ASSISTANT RESEARCH OFFICER: FOR CHAIRPERSON
AFRICA UNIVERSITY RESEARCH ETHICS COMMITTEE

Appendix 2: Questionnaire

Introduction:

Your participation in this research study on Zimbabwe's infrastructure and cybersecurity readiness is appreciated. The purpose of this survey is to obtain insightful information from those who are active in the nation's digital economy. Your answers are private and will only be utilized in conjunction with this study.

Part 1: General Information

1. Which sector or role is your main one?

    - Academic institution
    - Private sector company
    - Public sector organization
    - Government agency
    - Other (Please indicate)

2. What level would you place your cybersecurity experience

    - Beginner
    - Intermediate
    - Advanced

3. Does your company have a formal cybersecurity policy or structure in place?

    - Yes
    - No
    - Unsure

Part 2: Cybersecurity Practices

A. Awareness and Training

1. Have you received cybersecurity awareness training from your organization?
   - Yes
   - No
2. If yes, how often do you receive such training?
   - Never
   - Annually
   - Bi-annually
   - More frequently
3. Do you think the offered training covers current cybersecurity threats and is sufficient?
   - Strongly Agree
   - Agree
   - Neutral
   - Disagree
   - Strongly Disagree

B. Policies and Procedures

1. Does your company have a designated individual or team that handles cybersecurity?

- Yes
- No
- Unsure

2. Are there explicit guidelines and protocols concerning:
    - Management of passwords (Yes/No/Unsure)
    - Control and access of data (Yes/No/Unsure)
    - Reporting incidents (Yes/No/Unsure)
    - Security of mobile devices (Yes/No/Unsure)

C. Technology and Infrastructure

1. Does your company use anti-malware software, intrusion detection systems, or firewalls as security measures?
    - Yes
    - No
    - Unsure
2. To what extent do you think the IT infrastructure of your company is secure overall?
    - Very confident
    - Somewhat confident
    - Neutral
    - Somewhat concerned
    - Very concerned

Part 3: Improving Cybersecurity Infrastructure

1. What obstacles do you think stand in the way of Zimbabwe's effective cybersecurity? (Please select all that apply)
    - Lack of awareness and training
    - Limited resources (financial, technical manpower)
    - Outdated infrastructure
    - Inadequate legal framework
    - Other (Please specify)
2. What particular steps may the government or other public institutions do to strengthen their cybersecurity framework?
    - (Open ended question)
3. Do you have any additional comments or suggestions regarding cybersecurity in Zimbabwe?
    - (Open ended question)

Appendix 3: Informed Consent

My name is Tampiwa Mahari, a final year Computer Science student from AU. I am carrying out a study on Assessment of Zimbabwe's Cybersecurity Readiness And Infrastructure I am kindly asking you to participate in this study by filling in the google form questionnaire.

What you should know about the study:

Purpose of the study:

The purpose of the study is to identify the effectiveness of cybersecurity practices in Zimbabwe and to identify ways of improving cybersecurity infrastructure in government and public institutions. You were selected for the study because your organization and line of business is directly affected by effectiveness of cybersecurity practices.

Procedures and duration

If you decide to participate you will be expected to answer the questions on the form to the best of your ability It is expected that this will take about 15 minutes of your time.

Risks and discomforts

You may feel reluctant to talk about the cybersecurity practices at your organization and you may feel like you are putting your security at risk.

Benefits and/or compensation

There are no tangible benefits or compensation being given to anyone that takes part in the research study.

Confidentiality

Your participation in this research study is completely voluntary. All information you provide will be kept confidential. This means that any details that could identify you will not be disclosed without your written permission. We will not ask for your name or any other identifying information in the questionnaire.

Voluntary participation

Participation in this study is voluntary. If participant decides not to participate in this study, their decision will not affect their future relationship with Africa University If they chose to participate, they are free to withdraw their consent and to discontinue participation without penalty.

Offer to answer questions

Before you sign this form, please ask any questions on any aspect of this study that is unclear to you. You may take as much time as necessary to think it over.

Authorization

If you have decided to participate in this study, please sign this form in the space provide below as an indication that you have read and understood the information provided above and have agreed to participate.

-- ------------------------------

Name of Research Participant (please print) Date

Signature of Research Participant or legally authorised representative

If you have any questions concerning this study or consent form beyond those answered by the researcher including questions about the research, your rights as a research participant, or if you feel that you have been treated unfairly and would like to talk to someone other than the researcher, please feel free to contact the Africa University Research Ethics Committee on telephone (020) 60075 or 60026 extension 1156 email aurec@africau.edu

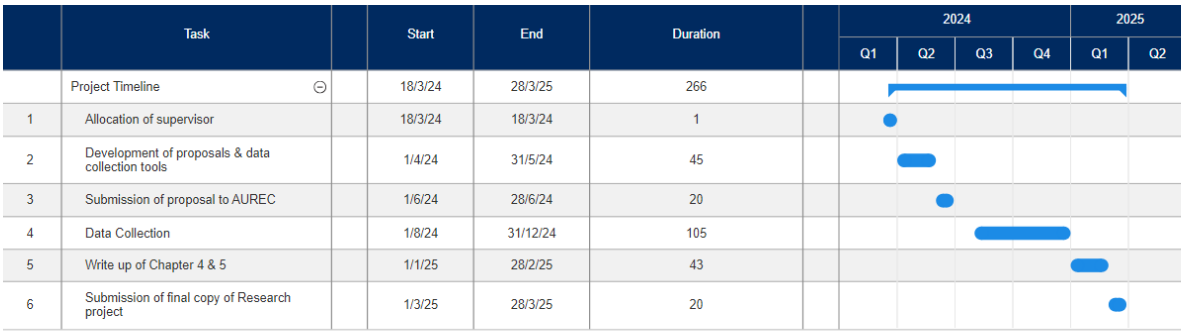
Name of Researcher
Tampiwa Mahari

Appendix 4: Project Budget

	ACTIVITY	COST (US$)
1	Research Materials and Software	50
2	Communication and Internet	20
3	Printing and Stationery	10
4	Miscellaneous Expenses	50
TOTAL		130

Table 4-Project Budget

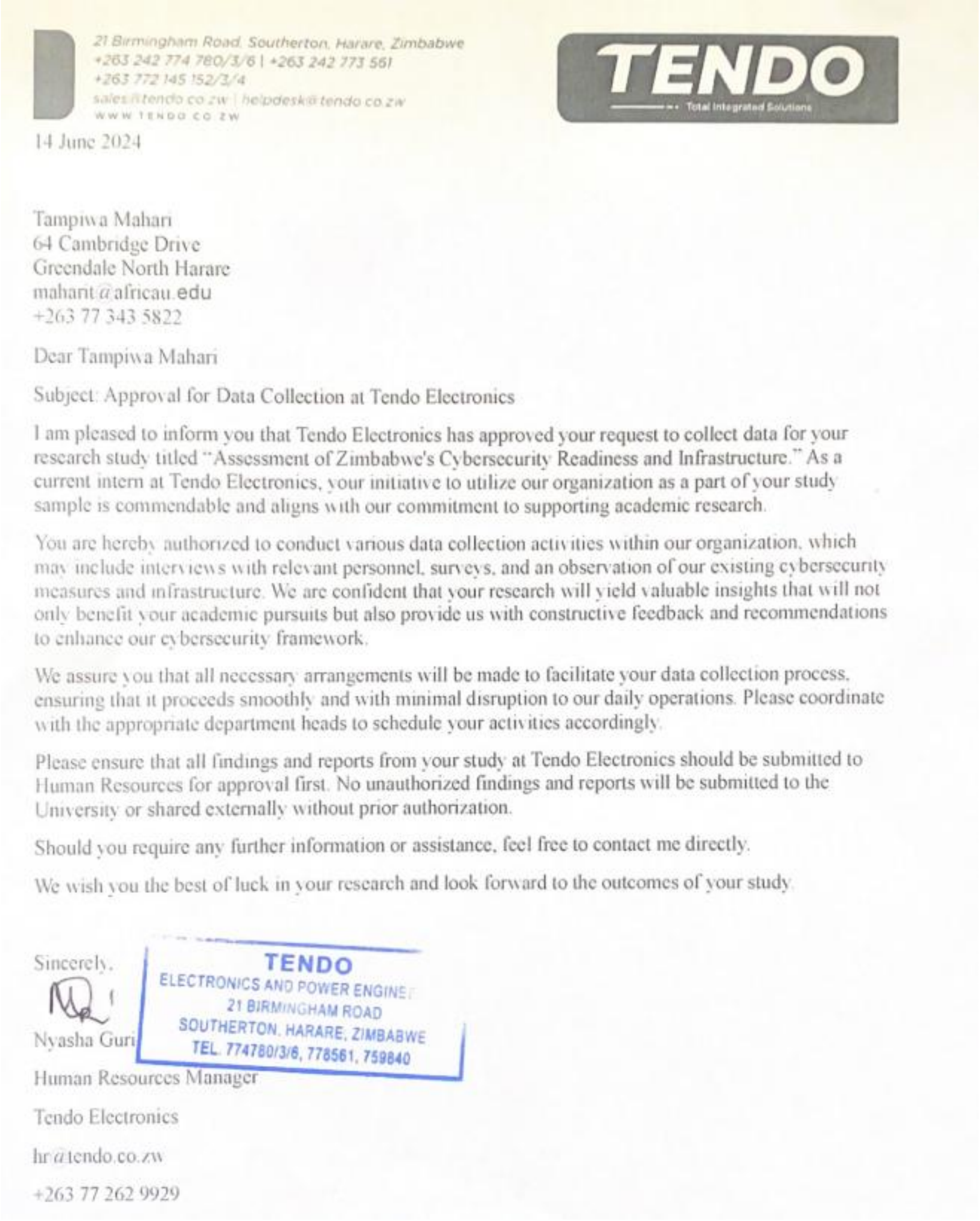
Appendix 5: Project Timeline



	Task	Start	End	Duration
	Project Timeline	18/3/24	28/3/25	266
1	Allocation of supervisor	18/3/24	18/3/24	1
2	Development of proposals & data collection tools	1/4/24	31/5/24	45
3	Submission of proposal to AUREC	1/6/24	28/6/24	20
4	Data Collection	1/8/24	31/12/24	105
5	Write up of Chapter 4 & 5	1/1/25	28/2/25	43
6	Submission of final copy of Research project	1/3/25	28/3/25	20

Figure 15-Gantt Chart

Appendix 6: Approval for Data Collection



21 Birmingham Road, Southerton, Harare, Zimbabwe
+263 242 774 780/3/6 | +263 242 773 561
+263 772 145 152/3/4
sales@tendo.co.zw | helpdesk@tendo.co.zw
www.tendo.co.zw

TENDO
Total Integrated Solutions

14 June 2024

Tampiwa Mahari
64 Cambridge Drive
Greendale North Harare
maharit@africau.edu
+263 77 343 5822

Dear Tampiwa Mahari

Subject: Approval for Data Collection at Tendo Electronics

I am pleased to inform you that Tendo Electronics has approved your request to collect data for your research study titled "Assessment of Zimbabwe's Cybersecurity Readiness and Infrastructure." As a current intern at Tendo Electronics, your initiative to utilize our organization as a part of your study sample is commendable and aligns with our commitment to supporting academic research.

You are hereby authorized to conduct various data collection activities within our organization, which may include interviews with relevant personnel, surveys, and an observation of our existing cybersecurity measures and infrastructure. We are confident that your research will yield valuable insights that will not only benefit your academic pursuits but also provide us with constructive feedback and recommendations to enhance our cybersecurity framework.

We assure you that all necessary arrangements will be made to facilitate your data collection process, ensuring that it proceeds smoothly and with minimal disruption to our daily operations. Please coordinate with the appropriate department heads to schedule your activities accordingly.

Please ensure that all findings and reports from your study at Tendo Electronics should be submitted to Human Resources for approval first. No unauthorized findings and reports will be submitted to the University or shared externally without prior authorization.

Should you require any further information or assistance, feel free to contact me directly.

We wish you the best of luck in your research and look forward to the outcomes of your study.

Sincerely,

TENDO
ELECTRONICS AND POWER ENGINE
21 BIRMINGHAM ROAD
SOUTHERTON, HARARE, ZIMBABWE
TEL. 774780/3/6, 778561, 759840

Nyasha Guri

Human Resources Manager

Tendo Electronics

hr@tendo.co.zw

+263 77 262 9929

Appendix 7: Proof of Payment of Review Fees

Ecobank Domestic transfer to 5783600003426 is successful with ref no 2653448317