THE CATHOLIC UNIVERSITY OF ZIMBABWE

FACULTY OF COMMERCE, INNOVATION AND TECHNOLOGY

DEPARTMENT OF INFORMATION TECHNOLOGY

DEVELOPING A CYBERSECURITY FRAMEWORK FOR MITIGATING RANSOMWARE AND INSIDER THREATS IN ZIMBABWE'S MINING SECTOR

BY

BRIGHTON GEZANI

PG247085H

SUPERVISOR: DR F. MASIMBA

A DISSERTATION SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE MASTERS IN BUSINESS MANAGEMENT AND INFORMATION TECHNOLOGY DEGREE.

26 FEBRUARY 2026

DISSERTATION RELEASE FORM

THE CATHOLIC UNIVERSITY OF ZIMBABWE

STUDENT: Brighton Gezani **I.D No:** 49-098832V49

Title of the dissertation: DEVELOPING A CYBERSECURITY FRAMEWORK FOR MITIGATING RANSOMWARE AND INSIDER THREATS IN ZIMBABWE'S MINING SECTOR

I certify that the above named student was under my supervision. I further certify that I have sufficiently supervised him and that he has fulfilled all the requirements that I set before him as a supervisor.

In my professional judgement, the dissertation is of sufficiently high standard to meet the standards of Masters in Business Management and Information Technology Degree as offered at The Catholic University of Zimbabwe. Hence I give The Catholic University of Zimbabwe permission to produce copies for this project and also reserve the author's publication rights.

Name of supervisor: DR. F. MASIMBA

Signature…  **…….** **Date: …**19/06/2026**…….**

APPROVAL FORM

The undersigned certify that they have read and recommended to The Catholic University of Zimbabwe or acceptance of the dissertation entitled, "Developing A Cybersecurity Framework for Mitigating Ransomware and Insider Threats in Zimbabwe's Mining Sector", submitted by Brighton Gezani in the partial fulfilment of the requirements for the Masters in Business Management and Information Technology degree.

.

Supervisor **Signature**

Dr. F. Masimba …… ……

Chairperson **Signature**

……..

DECLARATION

I, Brighton Gezani, declare and certify that this paper is entirely my own work and an accurate representation of the research I conducted. This research, in whole or in part, has not been submitted for any degree examination at any university.

_26/02/2026__ _  __19/06/2026__

_____

Student signature Date Supervisor Date

Dedication

I dedicate this dissertation to my beloved children; Brighton (Jnr), Liam and Eliana.

Abstract

Zimbabwe mining sector has been digitized resulting in improved operational performance but at the same time an increased vulnerability to ransomware and insider threats. With the integration of interconnected operational technology and enterprise systems, cybersecurity threats have become more devastating and destructive, especially to the mining organizations. The paper is a formulated integrated framework towards mitigating ransomware and insider threats in the Zimbabwe mining industry. Quantitative research design was used with data gathered on mining professionals at technological and managerial levels. The analysis of data was done to reliability testing, descriptive statistics, correlation analysis, and multiple regression modelling. Regression model was found to have a high explanatory power as it explained 52 percent of the variance in the exposure to cyber incidences. The results indicate that the most effective predictor of less incident exposure is governance maturity, in turn, ransomware preparedness, security awareness, insider threat mitigation, and technological control maturity. The findings prove that socio-technological integration, and not technology protection alone, is the basis of cybersecurity resilience in the mining setting. The mitigation of ransomware and insider threats involves the congruence of executive oversight, systematic preparedness systems, behavioral maturity, insider access control, and enhanced technological controls. Based on these results, the paper suggests the Mining Industry Ransomware and Insider Threat (MIRIT) Framework; it is a layered and governance-oriented framework adapted to an industrial setting. The research marks a contribution to the empirical data on the state of the mining industry in a developing economy and provides a practical proposal on how to make cybersecurity robust. Future studies must focus on longitudinal application of the framework and investigate adaptive strategies on cybersecurity in changing industrial threat environments.

Acknowledgements

I wish to express my sincere gratitude and appreciation to my supervisor, Dr. F Masimba and Millicent Mugwenhi whose input helped to produce a dissertation of good standard.

Contents

List of Figures

List of Tables

CHAPTER 1: Introduction

Zimbabwe's mining sector has been diving fast into digital technology over the last few years. This shift brings a lot of good, faster operations, better data, smoother decision-making. But this also opens the door to more complex and dangerous cybersecurity threats (Kaur et al., 2023). Ransomware is now a huge headache for the industry. It stops production, bleeds money, trashes reputations, and leaks sensitive data (Lawall and Beenken, 2024). It is not just outside hackers but people on the inside, whether they mean harm or just make mistakes keep making things worse. Insider actions often give ransomware a way in (Clifton, 2024). When we add all that up, mining companies in Africa, already working with tight resources, face difficulties in maintaining systems safe from cyber threats.

Even though mining is a so significant for Zimbabwe's economy, most companies do not have cybersecurity plans that really fit their environment. Cybersecurity maturity is all over the place. Lots of mines are stuck with old systems, not enough skilled people, limited budgets, and patchy security (Maphosa, 2024). Many just lean on big, generic frameworks like ISO 27001 or NIST. Those are solid for a baseline, but they do not really reflect the actual realities or unique setup of mining in developing countries (Safitra et al., 2023).

This study, therefore, is set out to build a cybersecurity framework that works for Zimbabwe's mines, something that tackles ransomware and insider threats by pulling together technological fixes, organizational changes, and human factors to enhance cyber resilience.

1.1 Background of the Study

Mines all over the world have been rushing to digitize, hoping for better efficiency, productivity, safety, and tighter control over costs. Automation is everywhere, cloud platforms are common, and new technology has made it way easier to see What is happening in real time. But with all this interconnectivity comes a much bigger attack surface for cybercriminals (Kaur et al., 2023).

As mining companies get more plugged in, cyber threats are hitting harder and more often. Ransomware stands out as one of the worst. These attacks do not just lock up data, they steal it, double or triple extort companies and can keep systems down for ages. That means lost production, big money losses, and a dented reputation (Lawall and Beenken, 2024). In mining, where you cannot afford to stop the machines, ransomware can bring everything to a standstill, mess with safety controls, and throw supply chains into chaos (Ibiyemi and Olutimehin, 2024).

Insider threats do not go away, either. Sometimes it is someone with bad intentions, sometimes just someone being careless. Employees, contractors, or third parties with legitimate access can all trigger problems, even if they do not mean to (Clifton, 2024). Research shows insider risks are not only about technology, but they are also shaped by how people act, the company culture, how things are managed, and what controls are in place (Saeed et al., 2023; Alsowail and Al-Shehari, 2022). In mining, where people and old technology must work together, these human-technology issues are even more obvious.

Back in Zimbabwe, mining is crucial for the economy, for bringing in foreign currency, and for jobs. Lately, local mining outfits have been rolling out more digital tools to modernize and stay competitive. But studies show cybersecurity in Zimbabwe is patchy companies often lack the skills, cash, and updated systems to really protect themselves (Maphosa, 2024). All of this makes it tough for mines to put strong cybersecurity in place.

A lot is changing in the world of cyber threats, but many mining companies in Zimbabwe still stick with old, piecemeal security measures and compliance-focused routines. Most of them lean on international standards like ISO 27001 and NIST as their main guides. Sure, these frameworks offer some solid basics, but research shows they usually miss the mark when it comes to the unique challenges in developing countries especially in industries like mining, where operational technology, people, and tight budgets shape the real risks.

This disconnects leads to a familiar problem: the official cybersecurity policies look good on paper, but the actual day-to-day security usually falls short.

There is another issue too. Traditional frameworks focus mostly on technology solutions and management structures, but they do not pay enough attention to human behaviour and

organizational habits. That is a big deal in mining, where things like insider actions, work pressure, and company culture have a direct impact on security. Add to that the gap between IT and OT security, and there is a recipe for trouble, especially when it comes to ransomware and insider threats that these frameworks just are not built to handle.

All of this points to a glaring problem in Zimbabwe's mining sector: there is no cybersecurity framework built for its specific needs, one that tackles ransomware and insider risks while also considering how the industry works, where people and limited resources play such big roles. What is needed is a tailored approach that mixes technology, organizational, and human-focused controls, all matched to the real risks miners face. This study aims to fill that gap by building a cybersecurity framework designed to help Zimbabwe's mining companies defend against ransomware and insider threats, so they can boost their cyber resilience and manage security more effectively.

1.2 Research Problem

Zimbabwe's mining industry is going through a rapid digital overhaul. Companies rely more on connected operational technology, enterprise systems, and cloud platforms to keep things running, that is from production and logistics to financial management. This digital expansion has opened the door to more cyber threats, especially ransomware, which has been hitting Africa hard lately and causing serious disruptions, heavy financial losses, and costly downtime. At the same time, insider threats, whether it is careless employees, stolen credentials, or people acting with bad intentions, remain tough to handle because those insiders have legitimate access to critical systems and environments.

Reports like the Verizon Data Breach Investigations Report (2023) make it clear: human actions and insider mistakes or sabotage do not just help ransomware get in but they often make things worse. That means the sector needs new, integrated ways to fight these threats. But despite all this, Zimbabwe's mining companies still rely on scattered security controls, outdated monitoring, and generic frameworks like ISO 27001 and NIST. These just do not fit the real-world challenges, resource limits, or the unique mix of people and technology in mining.

That leaves the sector with a major vulnerability. What is missing is a cybersecurity framework built around the realities of Zimbabwe's mining industry, one that works against both ransomware and insider threats.

1.3 Research Objectives

1. To identify the current cybersecurity measures used by selected mining organizations in Zimbabwe in relation to cyber threats.
2. To analyze the key factors that contribute to cybersecurity vulnerabilities in the mining sector.
3. To evaluate the effectiveness of existing mitigation strategies used in Zimbabwe's mining sector to address insider threats.
4. To design a practical, context-specific cybersecurity framework that integrates cybersecurity control measures tailored for Zimbabwe's mining sector.

1.4 Research Questions

1. What cybersecurity measures are currently implemented by mining organizations in Zimbabwe to address cyber threats?
2. What factors contribute to mining-sector vulnerability to insider-driven security breaches in Zimbabwe?
3. How effective are the existing mitigation strategies controls used in Zimbabwe's mining sector in managing insider-threat risks?
4. What key components should be included in a context-specific cybersecurity framework for mitigating insider threats that leads to ransomware attacks in Zimbabwe's mining sector?

1.5 Significance of the Study

This study matters a lot to anyone involved in mining or cybersecurity, especially in Africa. There is not much research done on cybersecurity threats in Africa's heavy industries, so this work fills a real gap. This study takes a close look at both ransomware and insider threats in Zimbabwe's

mining industry. By tackling both at once, the research paints a fuller picture of what mining companies are up against.

But it does not stop at just identifying risks. The study rolls out a cybersecurity framework built for Zimbabwe's unique environment, where resources are tight and challenges are different. This framework digs into how technology, human behaviour, and organizational choices all mix to shape cyber risk. For mining organizations, it is a practical guide of spotting the weak spots, building strong defences, and putting smart policies in place to deal with threats from outside and within.

A key point here is the focus on insiders. Whether it is carelessness or something more sinister, insider actions often open the door to ransomware. The study gets into strategies that blend technological fixes with efforts to shape employee behaviour, so companies are not just relying on one approach.

This is not just useful for companies, though. Regulators, policymakers, and cybersecurity professionals also get something out of it. The research calls out vulnerabilities specific to mining and offers recommendations grounded in real evidence. That means national policies, best practices, and industry standards can all get a boost from what is in this study. In the end, it is about making mining operations tougher in protecting vital resources, and cutting down on the damage cyber threats can cause for Zimbabwe's mining sector.

1.6 Scope and Limitations

This study zeroes in on one thing, building a cybersecurity framework to tackle ransomware and insider threats in Zimbabwe's mining industry. It looks at how governance, preparedness for ransomware, insider threat controls, security awareness, and technological strength all affect how exposed companies are to cyber incidents. The research draws on survey data from mining professionals, staff in IT, cybersecurity, and management.

There are some boundaries on how this study only looks at formal mining organizations in Zimbabwe. It does not cover other industries like banks, hospitals, or government agencies. While the findings might ring true for similar industries, they do not claim to cover every sector or mining operations outside Zimbabwe, especially where rules or technologies are different.

Method-wise, it is a cross-sectional study, which means it captures data at one point in time. It does not track changes over months or years. Plus, it depends on what people report in surveys, so there is always a chance for bias or different interpretations.

The statistical model explains a lot about why some companies face more incidents than others, but it does not touch on everything. Things like how national laws are enforced, the complexity of supply chains, or how advanced the technology infrastructure is are some factors that are not part of the analysis.

Even with these limits, the study offers a focused, real-world look at how Zimbabwe's mining sector can fight back against ransomware and insider threats.

1.7 Structure of the Dissertation

This dissertation has six chapters.

Chapter 1 kicks things off with the background, what problem the research tackles, the main objectives and questions, why it matters, what is covered (and what is not), plus a quick roadmap of what is coming up.

Chapter 2 dives into the literature. Here, the study looks at the big theories, socio-technological systems and risk management and dig into what other researchers have found about ransomware, insider threats, cybersecurity governance, and digital transformation in industry. The section spells out where the current research falls short and lays the groundwork for the MIRIT Framework.

Chapter 3 goes into how the research was conducted. It talks about the overall design, who was studied, how the data was collected, which statistical tools were used, and the ethical rules that were followed. This chapter also explains why these choices were made and how main ideas were tested.

Chapter 4 is all about what the data says. This is where response rates are shown, who participated, whether the measures were reliable, and all the key statistics like correlations and regression of results. This chapter also checked the research hypotheses and shows how things like governance, preparedness, insider mitigation, awareness, technological controls, and incident exposure all connect.

Chapter 5 puts the results under the microscope. It digs into what the findings mean in real-world and theoretical terms, talk about what this adds to what we already know, highlight what business and IT professionals can take away, and admit where the study has its limits.

Finally, Chapter 6 wraps it all up. This chapter sums up the main findings and draws some final conclusions. Practical advice for mining companies that want to boost their cybersecurity and some thoughts on where future research could take the MIRIT Framework is explained.

CHAPTER 2: Literature Review

2.1 Introduction to Key Concepts

Digital transformation is changing the face of industry, and with it, the nature of cybersecurity threats. Mining, once all about heavy machinery and physical systems, now leans heavily on both IT and operational technology (OT). This shift brings a boost in efficiency and competitiveness, but it also opens the door to a different breed of cyber risks, especially ransomware attacks and insider threats.

Ransomware is not just about locking up files anymore. Attackers now often steal data and use multiple forms of extortion to ramp up the pressure on victims. Mining operations, with their need for constant uptime and strict safety standards, are particularly vulnerable.

Then there are insider threats. These come from people inside the organization. These are employees or contractors who already have access to systems and data. Sometimes it is malicious, sometimes it is just carelessness or an honest mistake. Either way, the problem goes beyond technological flaws. Recent studies point out that insider threats are really about people, culture, and how organizations are run, not just gaps in software or hardware.

To tackle these risks, companies use different cybersecurity frameworks. Still, most industrial workplaces, especially in developing economies, try to fit their unique challenges into generic, global standards like ISO 27001 and NIST but that is starting to change. There is a growing realization that mining (and similar sectors) needs tailored frameworks that blend technological defences with human and organizational controls.

This chapter takes a close look at the theories and research behind building a cybersecurity framework for mining operations in Zimbabwe, focusing on how to deal with ransomware and insider threats.

2.2 Theoretical Framework

Creating a solid cybersecurity framework for mining means building on proven theories. Here, the main foundations are Socio-Technological Systems Theory, Defense-in-Depth, and Risk Management, with some extra insight from technology adoption models.

2.2.1 Socio-Technological Systems Theory

Socio-Technological Systems Theory says that what happens in an organization comes from the way people, structures, and culture mix with tools, processes, and technology. In cybersecurity, the real risk is not just a technological glitch, but it is when human behaviour and system design do not line up.

Insider threats, for example, often exploit weak spots like poor management, low cybersecurity awareness, or unclear job roles. In industrial settings, people and machines work side by side, making everything more tangled and complex. That is why it is not enough to just rely on technological fixes. Human-focused controls, good policies, regular training, clear accountability, and a strong organizational culture are just as important as firewalls or passwords. Any effective cybersecurity approach must treat them that way.

2.2.2 Defense-in-Depth Theory

Defense-in-Depth is basically about layering defenses, technological, administrative and physical, so there is no reliance on just one thing to ensure cyber security. If something slips through, there are still some further barriers to preventing an attack. Kaur et al (2023) put it bluntly: do not put your trust in any single defense. Lawall and Beenken (2024) saw that stopping ransomware gets a lot simpler when organizations combine privileged access management, solid monitoring, and regular user training. When these tools overlap, they cover the technology details, and the bigger governance issues the framework tries to solve.

2.2.3 Risk Management Theory

Risk Management Theory is straightforward: spot the risks, figure out which ones really matter, and tackle them. It is about weighing how likely each threat is and how much it could hurt. For industries on a shoestring budget like Zimbabwe's mining sector, prioritizing by risk means one gets more out of every cybersecurity dollar (Safitra et al., 2023). There is plenty of research backing this up. When organizations let risk drive their strategy, they come out stronger, especially against things like ransomware and insider threats (Ibiyemi and Olutimehin, 2024).

2.3 Review of Relevant Literature

2.3.1 Global Growth of Digitalization and Expanding Cyber Risk

Cloud computing, automation, data analytics, and the Internet of Things are shaking up how organizations run, everywhere. Sure, they make things faster and more efficient, but they also ramp up cyber risk (Saeed et al., 2023; Accenture, 2024). Researchers keep pointing out the danger: connecting old Operational Technology with modern IT systems, especially in industrial settings, just opens the door to more problems (Jain and Kotecha, 2023; Khan et al., 2024).

Ransomware is still the top cyber nightmare. Attackers have become so sophisticated too. Instead of casting a wide net, they aim straight at targets that cannot afford downtime. And now, with Ransomware-as-a-Service (RaaS), anyone even without deep technology skills can launch sophisticated attacks (Lawall and Beenken, 2024; Broadhurst et al., 2024). Industries that have to stay up 24/7 like mining, manufacturing, critical infrastructure, are prime targets, since attackers know these groups are more likely to pay just to keep running (IBM Security, 2024; Richardson and North, 2023).

Insider threats are on the rise, too, mostly because of human mistakes and bad security habits. It is not always sabotage but sometimes it is just someone being careless or not following basic security steps (Greitzer et al., 2023; Alsowail and Al-Shehari, 2022). The numbers say it all: insiders can help outsiders without even knowing it, maybe by messing up passwords, misconfiguring systems, or falling for phishing scams (Clifton, 2024; Verizon, 2024). Some recent studies even show insider mistakes and ransomware often go together (Nurse et al., 2024; Ponemon Institute, 2023).

All these technological and human gaps just make it clearer that we need cybersecurity frameworks that blend both social and technological angles, like those based on socio-technological theory and defense-in-depth (Safitra et al., 2023; ENISA, 2023). But even now, researchers say most frameworks still do not match up with the real-world challenges faced by sectors with tight budgets or unique needs (Obi et al., 2024; Goni et al., 2023).

2.3.2 Industrial Digitalization and Emerging OT/ICS Vulnerabilities

Industrial sectors like mining, energy, and manufacturing now depend more than ever on OT systems like SCADA, PLCs, and distributed control. These setups used to run on their own, totally separated from IT networks but not anymore. Companies have started connecting everything for automation, predictive maintenance, and centralized control (Elmrabit et al., 2024; Kaur et al., 2023). Digitalization boosts productivity, but it also opens the door to more cyber-attacks. A lot of these OT systems run on old architectures that focus on keeping things running, not on keeping things secure. So once plugged into outside networks, they become easy targets (Moussaileb et al., unpublished manuscript; Kaspersky, 2023).

Studies show cyberattacks on Industrial Control Systems (ICSs) have spiked worldwide. In 2023, more than a third of ICS setups faced some kind of malicious activity (Kaspersky, 2023). Researchers point to the same culprits, outdated components, weak authentication, insecure protocols, and patching headaches) (Jain and Kotecha, 2023; Khan et al., 2024).

There is another problem of digitalization in extractive industries, which is moving way faster than their cybersecurity measures can keep up. That is leaving gaps for attackers to slip through (Chikosha and Mhlanga, 2023; Oluwafemi et al., 2024). When OT-specific security controls are missing, monitoring is not continuous, and IT and OT networks are not properly separated, the risk of ransomware and insider threats just keeps climbing (ENISA, 2023; Tembo and Phiri, 2024).

2.3.3 Ransomware as a Rising Threat in Industrial Sectors

Ransomware is not just growing but it is exploding, especially in industries where downtime is not an option (Richardson and North, 2023; Elmrabit et al., 2024). From 2023 to 2025, attackers have

gotten better at finding holes in these mixed IT/OT environments. They are using smarter tactics, like stealing credentials, abusing remote access, and utilizing social engineering (Lawall and Beenken, 2024; Moyo and Madi, 2023).

In industrial settings, ransomware attacks go way beyond just locking up data. They stop operations, steal sensitive information, and use multi-stage extortion schemes (Ransomware Reloaded, 2024). Studies point out how the fallout can be huge when equipment fails, production halts, and sometimes safety is on the line. Mining operations are sitting ducks for this kind of risk (Tembo and Phiri, 2024).

Detecting and stopping ransomware has been found not easy. Attackers use tricks like polymorphic malware, encrypted traffic, and fileless techniques to stay under the radar (Cryptographic Ransomware Encryption Detection Survey, 2024; Moussaileb et al., unpublished manuscript). That is why recent research pushes for behavior-based and machine learning-driven detection tools to keep up with these ever-changing threats (Kaur et al., 2023; Goni et al., 2023).

2.3.4 Insider Threats as a Growing Global Cybersecurity Concern

Insider threats are a real headache for every industry. Sometimes it is careless employees, sometimes it is someone with bad intentions, or maybe it is just compromised accounts. Behavioral research shows these threats often stem from stress, dissatisfaction, poor training, or weak policies (Greitzer et al., 2023; Clifton, 2024).

The trend is clear, insider incidents are on the rise, both in frequency and cost, according to the Ponemon Institute (2023). Negligence on the inside is especially dangerous because it gives outside attackers a free pass, often letting ransomware in through phishing or stolen credentials (Nurse et al., 2024; Alsowail and Al-Shehari, 2022).

Recent studies point out that fighting insider threats takes a layered approach: ongoing authentication, tighter privilege controls, and behavioral analytics all play a part (Clifton, 2024; Safitra et al., 2023). Since insider actions and ransomware attacks often overlap, there is a growing call for integrated strategies that tackle both at once (Obi et al., 2024; Saeed et al., 2023).

2.3.5 Africa's Cybersecurity Landscape

Africa's growing digital transformation is dragging all kinds of sectors from mining, energy, finance, to telecommunications, into new territory when it comes to cyber risk. More people and companies are operating online than ever, but the continent is not keeping pace with cybersecurity. The main issues are, not enough investment in cyber infrastructure, a serious shortage of skilled professionals, and policies that are not well crafted (Oluwafemi et al., 2024; Mhlanga, 2023). Recent threat intelligence makes it clear that African organizations are prime targets for ransomware gangs. Weak defenses, old systems, and big gaps in threat intelligence make them easy targets (Deloitte Africa, 2024; CSIR, 2023).

Academic research backs this up. Cybercriminals are zeroing in on vulnerabilities like ransomware, phishing, data breaches, and insider threats are all on the rise (Adu and Darko, 2023; Nurse et al., 2024). Mining and extractive industries get hit especially hard. Their digital upgrades have outpaced their ability to manage cyber risks, leaving holes in everything from IT/OT integration to access controls and basic security governance (Chikosha and Mhlanga, 2023; Tembo and Phiri, 2024).

Several recent studies point to the same problems. Saeed et al. (2023) say there is not enough sharing of threat intelligence between African organizations. Goni et al. (2023) highlights big gaps in user awareness, detection, and incident response. Kaur et al. (2023) adds that while new technology brings efficiency, it also creates brand-new attack routes that most African organizations are not ready for.

Put simply, research keeps showing that Africa's rush to go digital is not matched by solid cyber governance. That gap is putting critical sectors, especially mining, at ever greater risk.

2.3.6 Cyber Threats in Africa's Mining Sector

Mining sits at the heart of Africa's economy, and lately, it has been under fire from sophisticated cyber threats. As mining companies plug in IoT sensors, automate operations, and run some applications in the cloud, the number of ways hackers can break in goes high (Tembo and Phiri, 2024; Chikosha and Mhlanga, 2023).

Both researchers and industry experts agree on the main problems of many mines still depend on old OT/ICS systems, networks are not properly segmented, budgets for cybersecurity are low, and there are not enough cyber specialists available (Adu and Darko, 2023; Kaspersky, 2023). A ransomware attack can freeze production, mess up supply chains, wreck expensive equipment, and hit a company's finances and safety in a huge way (Richardson and North, 2023; Moyo and Madi, 2023).

Lawall and Beenken (2024) point out that ransomware syndicates go after high-value industries like mining because downtime costs so much to them and are more likely to pay up ransom. Ransomware Reloaded (2024) highlights the rise of "double-extortion" and data theft attacks in extractive industries. Moussaileb et al. (unpublished manuscript) show how today's ransomware uses sophisticated and stealth methods to slip past standard security measures in mining's control systems.

Then there is the insider threat. African mining sites rely on lots of contractors, outside service providers, and shifting crews. That mix raises the odds of stolen credentials, accidental data leaks, and people just not following the rules (Madzimure and Nyemba, 2024). Literature is clear that insiders, whether through social engineering, phishing, bad system setups, or risky behavior, are often the weak link that ransomware attackers exploit (Clifton, 2024; Alsowail and Al-Shehari, 2022).

The bottom line is cyber threats in Africa's mining sector keep getting worse. Digital advances are outpacing security measures, and insider risks are not being managed well enough to keep up.

2.3.7 Zimbabwe's Cybersecurity Environment

Zimbabwe's digital landscape is changing fast, but national cybersecurity still lags. The Cyber and Data Protection Act (2021) set up a basic framework for cybersecurity governance, but enforcement is weak. Sector-specific rules, especially for mining, are still missing (Mukucha and Mapuranga, 2024; Mhlanga, 2023). Zimbabwe does not have a fully functional National Computer Emergency Response Team (CERT), which means organizations struggle to coordinate incident response, share threat intelligence, or get early warnings.

Researchers point out that Zimbabwean organizations deal with tight budgets, old technology, and lack of skilled professionals, making it tough to improve cybersecurity (Oluwafemi et al., 2024; Adu and Darko, 2023). A lot of companies in Zimbabwe do not follow international cybersecurity standards like ISO 27001, NIST CSF, or IEC 62443, mostly because of competing priorities, high costs, and not enough expertise (Mukucha and Mapuranga, 2024).

Goni et al. (2023) found out that countries with weak cyber governance are slow to put even basic security measures in place. Safitra et al. (2023) stress the need for resilient frameworks where cybersecurity maturity is low. Obi et al. (2024) adds that without a strong security culture or enough awareness, an organization's defenses fall apart, especially in developing countries.

All in all, Zimbabwe's cybersecurity scene is marked by weak governance, scattered efforts, and not enough resilience. This leaves the mining sector exposed to greater risks.

2.3.8 Digitalization in Zimbabwe's Mining Sector

Mining is key to Zimbabwe's economy, and the industry is largely embracing digitalization to work smarter and faster. Companies now use automated systems, OT-driven processing plants, ERP systems, fleet management, and remote monitoring (Chikosha and Mhlanga, 2023).

Digitalization boosts productivity, but it also opens the door to new cyber risks if security does not keep up. Many mining companies still operate outdated systems with little to no modern security. Their OT and ICS setups often rely on unpatched software or old protocols (Tembo and Phiri, 2024; Kaspersky, 2023).

Insider threats are a big problem, too. Weak training, sloppy access control, shared passwords, and heavy use of contractors all make it easier for attacks to happen from the inside (Madzimure and Nyemba, 2024). Clifton (2024) points out that everyday negligence like using weak passwords or unsafe system habits fuels cyber incidents in Africa's industrial sectors.

Most mining organizations in Zimbabwe do not have their own cybersecurity teams or Security Operations Centers (SOCs), so they cannot spot things like ransomware movements, privilege escalation, or suspicious OT network traffic (Moussaileb et al., unpublished manuscript;

Cryptographic Ransomware Encryption Detection Survey, 2024). With these gaps, the mining sector faces serious threats from both ransomware and insider attacks.

2.3.9 Ransomware Trends in Zimbabwe's Industrial and Mining Sectors

There are limited publicly reported ransomware cases in Zimbabwe, probably because there is no rule forcing companies to disclose them. Still, research shows that ransomware is on the rise across different industries (Mukucha and Mapuranga, 2024). Mining companies are frequent targets for phishing, credential theft, and ransomware attacks, often linked to OT and ICS weaknesses (Tembo and Phiri, 2024).

Lawall and Beenken (2024) show that ransomware attackers go after operational vulnerabilities in industrial systems. Kaur et al. (2023) warn that AI-driven ransomware is getting smarter, making it harder for companies to catch attacks in time. Saeed et al. (2023) note that limited cyber threat intelligence in developing countries makes early detection even tougher.

With Zimbabwe's mining sector depending on nonstop production, ransomware is not just an inconvenience, but it is a huge operational and financial threat. Ignoring it risks major disruptions and heavy losses.

2.3.10 Insider Threats in Zimbabwean Organizations

Insider threats are on the rise across Zimbabwean industries. With more businesses turning to technology, weak security culture, low awareness, and poor enforcement of cybersecurity policies are leaving big gaps (Madzimure and Nyemba, 2024). Mining companies have it tough. They depend on rotating staff and contractors, so insider risk is high especially in OT and ICS environments where even a small mistake can cause serious damage (Chikosha and Mhlanga, 2023).

Research keeps coming back to the same thing of insider actions often being the doorway for ransomware. Clifton (2024) and Alsowail and Al-Shehari (2022) point out that simple mistakes like clicking on phishing emails, messing up system settings, or mishandling passwords are the

usual entry points for ransomware. Nurse et al. (2024) add that attackers now rely on compromised insider accounts to spread ransomware and move quietly through networks.

In Zimbabwe's mining sector, these problems only get worse with gaps in training, no real monitoring, shared passwords, and weak privilege management. With poor governance in the mix, the current setup is a recipe for frequent cyber-attacks.

2.3.11 Cyber Governance and Regulatory Challenges in Zimbabwe

Zimbabwe's approach to cybersecurity just has not kept up with its rapid digital growth. The Cyber and Data Protection Act (2021) was a start, but experts say it does not go far enough, especially for sectors like mining where IT and OT systems blend and bring unique risks (Mukucha and Mapuranga, 2024; Mhlanga, 2023). Unlike countries with established national CERTs, Zimbabwe still does not have a fully working cyber response system. There is no central place to coordinate threat intelligence, manage incidents, or enforce industry-wide rules (Oluwafemi et al., 2024).

Without strong regulatory enforcements, companies end up with inadequate cybersecurity policies. Controls are uneven, incident handling is not structured enough, and response plans are weak (Adu and Darko, 2023). Recent studies back this up. Goni et al. (2023) point out that, in developing economies, poor governance means best practices rarely take hold. Obi et al. (2024) show that when regulators do not keep watch, companies underinvest in cybersecurity. Safitra et al. (2023) argue that developing countries need resilience frameworks that tackle both resource shortages and policy gaps at once.

For mining, which is a backbone of Zimbabwe's economy, these regulatory gaps mean more exposure to ransomware and insider threats. Without required security standards, OT protection rules, or formal reporting mandates, organizations end up more vulnerable than they should be.

2.3.12 Organizational and Structural Cybersecurity Challenges in Mining

Inside Zimbabwe's mining sector, cybersecurity faces a challenge of internal problems. Many companies do not have a real cybersecurity strategy, a dedicated security team, or high-level oversight. So, security measures end up being reactive or thrown together on the fly (Mhlanga,

2023; Oluwafemi et al., 2024). Too often, firms treat cybersecurity as just another IT issue, not a company-wide risk. This mindset leaves big vulnerabilities in governance, responsibility, and resource allocation (Adu and Darko, 2023).

Budget constraints, skill shortages, and heavy reliance on outside contractors make things even tougher. These issues lead to inconsistent application of security measures (Chikosha and Mhlanga, 2023). In OT environments, that inconsistency can turn into system misconfigurations, unauthorized access, and mistakes that disrupt operations or endanger safety.

Clifton (2024) points out that organizations often ignore warning signs of insider threats, they do not monitor behavior closely, and do not control system access well. Alsowail and Al-Shehari (2022) show that without structured insider threat programs, companies are wide open to both careless and malicious insiders. Goni et al. (2023) and Saeed et al. (2023) highlight another big issue in places with limited resources, there is often no early warning system or continuous monitoring in place. Organizations only respond after an attack, instead of setting up proactive defenses.

With weak structures in place, mining firms end up unprepared for ransomware (like lacking network segmentation or incident response plans) and insider threats (like no behavioral controls, shared accounts, and poor auditing). It is a risky situation that needs urgent attention.

2.3.13 Risks Stemming from IT/OT Convergence in Zimbabwe's Mining Sector

When IT and OT systems come together in Zimbabwe's mining industry, they set the stage for one of the biggest new risks around. OT systems like machinery controls and plant operations used to be cut off from everything else. Their main job was to keep things running safely and reliably, not to fend off hackers. Now, as companies integrate these OT systems up to IT networks for automation, remote monitoring, IoT analytics, and centralized control, they drag in a lot of IT vulnerabilities that OT just is not built to handle (Jain and Kotecha, 2023; Elmrabit et al., 2024).

Academic research spells out the dangers that this merging of IT and OT makes OT systems targets for ransomware, stolen credentials, lateral movement, and remote hacks (Khan et al., 2024; Tembo and Phiri, 2024). Zimbabwean mining companies rarely separate IT and OT networks, so once an

attacker gets into the IT side, it is not hard to jump into OT systems too (Chikosha and Mhlanga, 2023).

Moussaileb and colleagues (unpublished manuscript) show that new ransomware strains are tuned to exploiting OT's weak spots. The Cryptographic Ransomware Encryption Detection Survey (2024) points out how slow, sneaky ransomware can slip past traditional OT monitoring tools. Meanwhile, Safitra et al. (2023) argue that OT governance needs to build in resilience, so cyberattacks do not grind operations to a halt.

It is not just about technology either. Zimbabwe's mining sector leans heavily on outside contractors, many of whom have remote system access. This opens new insider risks (Madzimure and Nyemba, 2024). Weak authentication, shared logins, and poor logging make it even easier for someone on the inside or someone pretending to be, to compromise OT systems.

2.3.14 Human Factor, Behavioral Risks, and Cultural Weaknesses

Human mistakes and risky behavior are at the heart of most cybersecurity incidents in industrial sectors worldwide. Research shows insider threats usually come down to carelessness, abusing access privileges, lack of training, stress, or sometimes just bad intentions (Greitzer et al., 2023; Clifton, 2024). In Africa, these problems get worse when resources are tight, cybersecurity culture, awareness, and user habits matter even more (Adu and Darko, 2023; Madzimure and Nyemba, 2024).

In Zimbabwean mining, insider risk is fueled by a mix of factors. Many companies do not run regular cybersecurity awareness training, policies are not enforced consistently, password habits are bad, and production always seems to come before cybersecurity. Shared passwords between local users and contractors only make things worse. High contractor turnover means lots of new people get access, yet there is almost no behavioral monitoring to identify problems.

Alsowail and Al-Shehari (2022) stress the importance of watching user behavior and using continuous authentication to cut down on insider threats. Ransomware studies (Lawall and Beenken, 2024; Goni et al., 2023) show that human error especially falling for phishing emails is

usually how ransomware sneaks in. Saeed et al. (2023) add that insider-driven leaks and misconfigurations often weaken security and open the door to attacks.

Since human behavior and ransomware are so tightly linked, weak security culture and poor habits stand out as major soft spots in Zimbabwe's mining operations. Companies need to close these gaps if they want to stand a chance against ransomware.

2.3.15 Cybersecurity Capacity Challenges in Zimbabwe

Zimbabwe has got a talent problem when it comes to cybersecurity. There aren't nearly enough trained professionals, especially those who know OT and ICS fully (Oluwafemi et al., 2024). Most mining companies do not have Security Operations Centers, threat-hunting teams, digital forensics, or proper incident response units (Mukucha and Mapuranga, 2024).

Audits show a lot of mining organizations run outdated antivirus software, do not monitor their networks, and let critical ICS components go unpatched (Tembo and Phiri, 2024). This makes it tough to catch ransomware early. Things like lateral movement, privilege escalation, or weird OT network activity often slip by (Kaspersky, 2023).

Resilience comes down to being able to anticipate, withstand, recover, and adapt to attacks but in developing countries, these skills are in short supply (Safitra et al., 2023). Saeed et al. (2023) point out that without cyber threat intelligence know-how, companies are slow to identify and respond to attacks.

All these capacity gaps just make Zimbabwean miners even more vulnerable to ransomware and insider threats. Building local skills and resources is not just a good idea but it is urgent.

2.4 Gap in Literature

Looking back at the literature, researchers have spent a lot of time on topics like ransomware, insider threats, cybersecurity governance, and digital transformation, especially in industrial settings. But even with all that attention, some important things are missing. For example, not much work digs into how these risks play out in specific places or sectors, like Zimbabwe's mining industry.

That's why a one-size-fits-all cybersecurity model does not really cut it here. What is needed is a framework that takes Zimbabwe's unique operational, regulatory, economic, and technology realities into account. This study aims to address that gap.

Ransomware has been addressed in global studies, but most of those focus on wealthier countries and high-technology industries like finance, healthcare, or government. These papers have taught us a lot about how ransomware evolves and how organizations can defend themselves, but they also tend to assume everyone has advanced detection tools, solid governance, and plenty of money to spend. That is just not the case in places like Zimbabwe, where companies face budget limits, skill shortages, and a mix of old and new technology systems. There is a real lack of research looking at how to deal with ransomware in industrial sectors that must make do with fewer resources.

Insider threats are another area that's been heavily studied, but again, most research focuses on big corporations or governments, focusing on technological monitoring and behavioural analytics. These studies are useful, but they often miss the bigger picture of things like governance maturity, workplace culture, or basic cybersecurity awareness, which are crucial in developing countries. Also, they tend to treat insider threats as totally separate from ransomware, even though stolen credentials from insiders are a common way for ransomware to get in. This split approach means organizations are not getting the integrated security strategies they really need.

When it comes to cybersecurity frameworks, the literature leans heavily on global standards like ISO 27001 or NIST. While these standards lay out good guidelines, evidence shows that in developing countries, organizations often just check the boxes for compliance without really changing how they operate. Some studies point this out, but they rarely offer grounded, sector-specific alternatives especially for sectors like mining, where things like IT–OT convergence, old infrastructure, and the need to keep systems running 24/7 are everyday challenges.

Studies on IT–OT convergence do highlight big vulnerabilities in industrial settings, but they're usually technological deep-dives that do not bring in governance or human factors. There is a real gap when it comes to integrated models that consider both social and technological sides, particularly for mining. Mining operations are different because they are spread out, rely on safety-critical machinery, and use a lot of automation. Yet there is not much research focused on these unique challenges.

There is also a big gap in how research is done. Most studies either run ransomware simulations or stick to conceptual governance analysis, but rarely combine real organizational practices, behavioural data, and incident records into a mixed-methods approach. That's a problem, especially in developing economies where theory and day-to-day reality often do not match up.

And, maybe most striking, hardly any research focuses directly on Zimbabwe's mining sector. Maphosa (2024) does a good job looking at cybersecurity in Zimbabwean finance, but mining is barely mentioned in national cybersecurity studies even though it is a backbone of Zimbabwe's economy and a key source of foreign currency.

So, looking at the research so far, one starts to notice four big gaps. First, there is just not enough attention to developing economies when it comes to studying ransomware and insider threats. Next, technological, behavioral, and governance approaches tend to stay in their own lanes instead of working together. Third, there is not much out there that's really tailored for specific sectors like mining. And finally, research often ignores how socio-technological and risk-based ideas play out in places where resources are tight. To fix this, a framework is needed that brings together technological controls, human-focused strategies, governance tools, and a way to prioritize risks specifically for Zimbabwe's mining industry.

This study strives to tackle those gaps adequately. It digs into how Zimbabwe's mining sector deals with ransomware and insider threats, and it comes up with a cybersecurity framework that fits the local context. The approach leans on ideas from socio-technological systems, defence-in-depth, and risk management. So, the study is not just adding to the conversation in theory, but it is also practical, giving developing economies something they can use.

2.5 The Proposed MIRIT Framework

From the literature review, there is a missing piece. No research has pulled together a sector-specific cybersecurity framework that really works for mining in developing countries. Plenty of research exists that looks at ransomware, insider threats, or governance, but rarely do these areas connect, especially in the context of industrial mining. This study, therefore, develops the Mining

Industry Ransomware and Insider Threat (MIRIT) Framework, which is a model built for the realities of Zimbabwe's mining sector, with governance at its core.

The MIRIT Framework rests on two main ideas: socio-technological systems theory and risk governance theory. Socio-technological theory is all about how technology, people, and the way organizations are set up all effect how things work (Saeed et al., 2023). Then there is risk governance theory, which points out how important leadership and clear policies are for keeping organizations safe (Safitra et al., 2023). When these theories are combined, MIRIT sees cybersecurity as a set of layers of organizational, behavioral, and technological that all work together.

There are five main parts to the MIRIT Framework: governance maturity, ransomware preparedness, insider threat mitigation, security awareness, and technological control maturity. Governance maturity comes first; it sets the tone and helps everything else work better. Ransomware preparedness covers planning, testing backups, and keeping systems separated. Insider threat mitigation is about controlling who has access and keeping an eye on systems. Security awareness is about how ready employees are to spot and respond to threats. And technological controls are the nuts and bolts that protect the infrastructure.

All these areas work together to predict how often and how badly a company gets hit by cyber incidents, especially ransomware and insider threats. The more mature each area is, the lower the risk of those incidents.

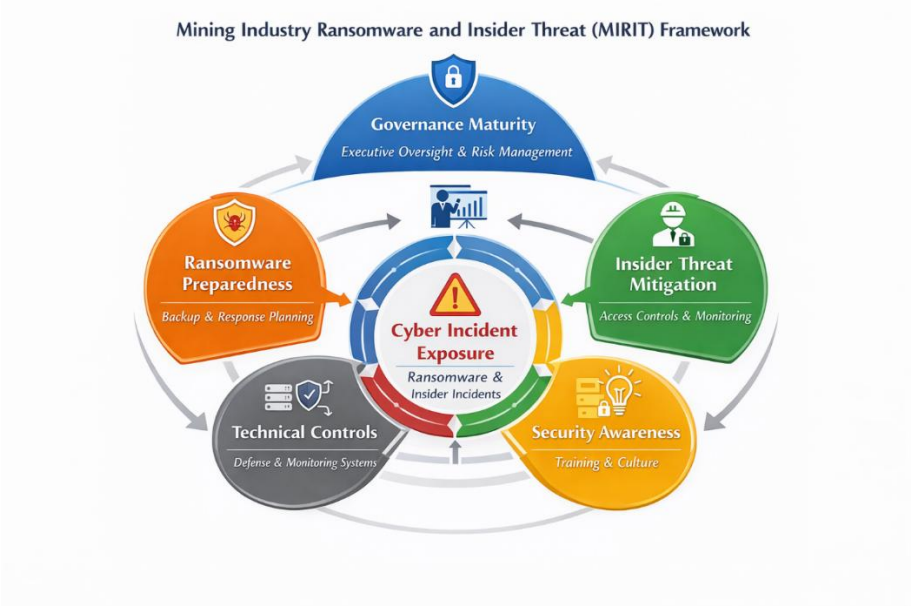

Figure 2.1: The Mining Industry Ransomware and Insider Threat (MIRIT) Framework

Based on the framework, the study proposes the following hypotheses:

H1: Ransomware preparedness is negatively associated with cyber incident exposure.
H2: Insider threat mitigation is negatively associated with cyber incident exposure.
H3: Technological control maturity is negatively associated with cyber incident exposure.
H4: Security awareness is negatively associated with cyber incident exposure.
H5: Governance maturity is negatively associated with cyber incident exposure.

The MIRIT Framework therefore serves as the conceptual foundation guiding the empirical investigation presented in subsequent chapters.

2.5 Summary

This chapter took a hard look at both the theory and real-world evidence behind building a cybersecurity framework to tackle ransomware and insider threats in Zimbabwe's mining sector. It started by digging into the basics, pointing out how digital transformation and cyber risk are now tightly linked especially in industries like mining. These companies lean more on connected

information systems and operational technology, which means they are exposed to a bigger risk of attacks. The mix of IT and OT, complicated systems, and tight budgets only makes things trickier.

To make sense of where these risks come from, the chapter leaned on Socio-Technological Systems Theory, Defense-in-Depth, and Risk Management Theory. The big takeaway is that cybersecurity risks do not just pop up because of technology flaws, but they grow out of how people behave and how organizations are run. So, fighting off ransomware and insider threats takes more than just plugging in some new software. There is need for layers of protection that work together and focus on the actual risks.

When it comes to business management, the review stressed how governance, strategy, company culture, and resources shape cybersecurity results. The evidence is clear that if a company has weak governance and people do not really get security, even the best technological controls will not hold up especially in countries where resources are already stretched. At the same time, the rush to digitalize, move to the cloud, and blend IT with OT makes companies more vulnerable if they do not step up their cybersecurity approach along the way.

Looking at ransomware, the literature shows how it has become a serious threat that can shut down operations and cause huge ripple effects across the economy. Research into insider threats points to the role of human mistakes and weak leadership in letting both malicious and careless breaches happen. Still, there is a clear gap: most research treats technological, organizational, and human factors as separate issues, without tying them all together.

There are some obvious gaps in what is out there. Not much research focuses on mining, especially in developing countries like Zimbabwe. What does exist often falls back on general compliance checklists that do not really fit the way resource-limited operations work. And there is a real lack of models that connect governance, human behavior, and technological controls into one practical approach.

All of this points to a big need of a cybersecurity framework that fits Zimbabwe’s mining sector, considering its unique economic, organizational, and technology realities.

This study fills that gap by building an integrated, risk-based, and socio-technological framework using real data from Zimbabwe's mining industry. The next chapter gets into how the research was carried out, laying out the methods used to study current cybersecurity practices and gathering the data needed to shape the final framework.

CHAPTER 3: Research Methodology

3.0 Introduction

This chapter covers the methods used to study cybersecurity practices in Zimbabwe's mining industry and how the Mining Integrated Ransomware and Insider Threat (MIRIT) Framework came to life. Every step ties back to the study's goals: checking how ready companies are for ransomware, looking at how they handle insider threats, evaluating both governance and socio-technological controls, and pinpointing what really predicts exposure to cyber incidents. Details on the research design, who was involved, how the data was collected and analysed, and the ethical rules that kept everything on track are the focus areas of this chapter.

With more mining operations going digital and facing more ransomware and insider threats, a structured, evidence-based approach was necessary. The methods chosen to make sure the framework is not just theory, but it is built on real data, statistically sound, and tuned to Zimbabwe's unique industrial setting.

3.1 Research Design

3.1.1 Philosophical Positioning

This study uses a positivist approach. That means treating organizational cyber practices as things can be measured, analysed, and understood through hard data (Saunders et al., 2019). The research aims to put numbers to cybersecurity maturity across different areas and see if those areas really affect how often companies get affected by cyber incidents. To do that, there is need to include things that can be measured and tested, which makes positivism a good fit.

The theoretical foundation of the study draws from socio-technical systems theory, defence-in-depth principles, and risk management theory. However, these theories require operationalisation into observable variables. A positivist approach allows for the translation of abstract constructs such as governance maturity and security awareness into quantifiable survey indicators.

3.1.2 Quantitative Cross-Sectional Design

The research uses a quantitative cross-sectional survey. Basically, this means collecting numbers and statistics at one point in time, across different mining companies. It is a way to see what is going on right now, compare companies, and spot patterns in their cybersecurity practices (Creswell, 2014).

This approach was used because companies work in fast-changing environments, and it is difficult to follow them for years. A cross-sectional snapshot works since it gives robust data for things like regression analysis and hypothesis testing, without dragging out data collection for a very long time.

This design also fits the study's aim of building the MIRIT Framework. To do that, there is need to know which factors most strongly predict cyber incidents. Quantitative data and regression analysis help zero in on the most important parts of the framework.

3.1.3 Conceptual Research Model

The research model is all about the idea that both technology and organizational factors shape cybersecurity outcomes. In Zimbabwe's mines, things like IT and OT systems merging, limited resources, and the local work culture all play a part.

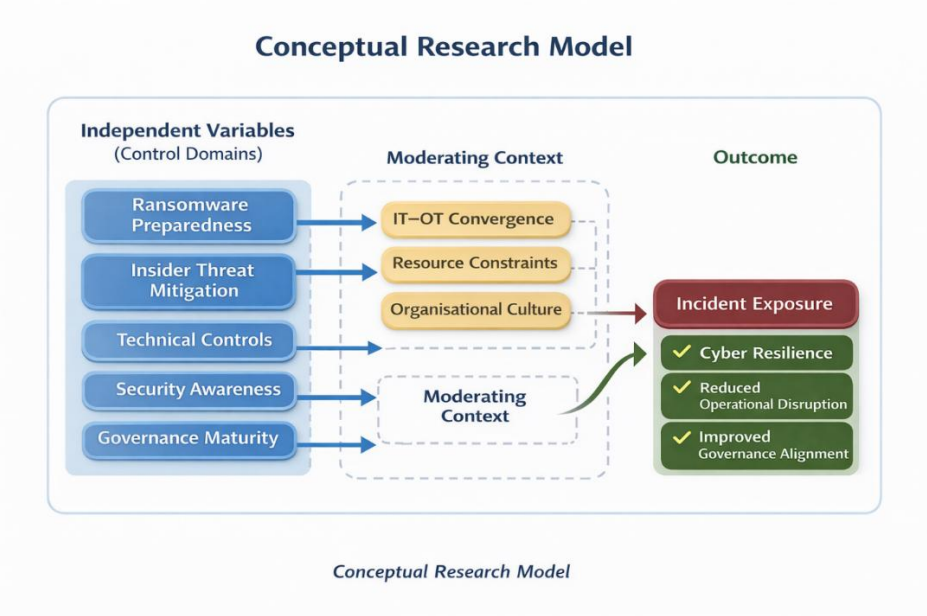

Figure 3.1: Conceptual Research Model

3.1.4 Hypothesis Development

After building the model and reviewing the literature, the study lays out these hypotheses:

H1: Better ransomware preparedness means fewer incidents.

H2: Stronger insider threat measures mean fewer incidents.

H3: Higher technological control maturity means fewer incidents.

H4: Higher security awareness maturity means fewer incidents.

H5: Better governance maturity means fewer incidents.

H6: Governance maturity makes technological controls even better at reducing incidents.

Previous research backs up these ideas, showing that a mix of technological and organizational controls really does cut cyber risks (Lawall and Beenken, 2024; Clifton, 2024; Safitra et al., 2023).

3.2 Population and Sample Selection

3.2.1 Target Population

The focus is on medium and large mining companies in Zimbabwe. This sector matters because it is a big piece of the economy, it is going through rapid digital change, and it depends heavily on interconnected IT and operational technology systems. These companies use automation, remote monitoring, enterprise platforms, and industrial control systems, all of which open the door to more cyber risks.

3.2.2 Unit of Analysis

This study focuses on people directly involved in cybersecurity governance, information systems management, operational technology, and organizational risk oversight. These are IT managers, cybersecurity officers, OT engineers, compliance staff, and top-level decision-makers. By bringing in a range of roles, the research captures both the technological and governance sides of the issue. Since insider threats and ransomware touch on organizational culture and strategy, management input plays a key role.

3.2.3 Sampling Strategy

This study used purposive sampling, choosing participants with specialized knowledge (Etikan et al., 2016). In cybersecurity, there is need for informed voices to ensure construct validity. Randomly picking people would mean including those without the necessary background, which weakens the results. While purposive sampling narrows generalizability, it strengthens internal validity in the mining sector. By reaching out to different mining organizations and professionals in varied roles, the study gets a more accurate picture at the sector level.

3.2.4 Sample Size Determination

Sample size was determined based on regression analysis needs. Tabachnick and Fidell (2013) recommend having enough cases for the number of predictors in the model. With five independent variables, we made sure to gather more than the minimum cases required for solid, reliable analysis.

3.3 Data Collection Methods

3.3.1 Instrument Development

The main tool was a structured questionnaire, built on established cybersecurity research. We based our constructs on previous work in ransomware mitigation (Lawall and Beenken, 2024), insider threat management (Clifton, 2024), and cyber governance (Safitra et al., 2023). Each construction was broken down into four Likert-scale items, measured on a five-point scale. The questionnaire stayed concise to keep participants engaged without sacrificing content validity.

3.3.2 Pilot Testing and Refinement

A pilot study with a group of cybersecurity professionals helped us test the questionnaire's clarity, wording, and internal consistency. Their feedback led to clearer items and a more logical flow. This step improved the instrument's reliability by refining item wording and confirming that the underlying constructs were clear and straightforward to interpret.

3.3.3 Survey Administration

We distributed the survey electronically through Google Forms. This digital approach made it easy to reach people across scattered mining sites. It also supported anonymity, automatic data collection, and smooth export to statistical software.

3.3.4 Secondary Data Integration

Secondary sources, including cybersecurity policies and risk documents, were consulted to validate survey responses and provide additional context. However, access varied considerably between organizations, and restricted document sharing limited the extent of documentary validation.

3.4 Data Analysis Technology

Data analysis was carried out in IBM SPSS Statistics using a staged process designed to support careful interpretation. We began with initial screening and data preparation before moving to multivariate modelling. These steps were applied to empirically assess whether the MIRIT Framework was supported by the data.

3.4.1 Data Screening and Preparation

Prior to the main analyses, the dataset was screened to confirm that it was suitable for statistical modelling. Response completeness was assessed, duplicate entries were identified and removed, and missing values were examined. Records with excessive missing data were excluded from further analysis. Where missingness was minimal and considered appropriate for imputation, mean substitution was used to address small gaps.

Outliers were assessed using boxplots and standardized z-scores (Field, 2018). Responses exceeding three standard deviations from the mean were flagged and reviewed to determine whether they reflected plausible extreme values or potential data entry errors. Multivariate outliers

were further evaluated using Mahalanobis distance, given the sensitivity of regression models to unusual combinations of predictor values.

Normality was assessed through multiple checks, including skewness and kurtosis statistics, visual inspection of histograms and Q–Q plots, and the Kolmogorov–Smirnov test (Field, 2018; Pallant, 2020). Although multiple regression is generally robust to modest departures from normality, substantial deviations were noted and considered when interpreting the results.

3.4.2 Measurement Model Assessment

Reliability and consistency of each construct were evaluated prior to the main analysis. Cronbach's alpha was calculated for Ransomware Preparedness, Insider Threat Mitigation, Technology Control Maturity, Security Awareness, Governance Maturity, and Incident Exposure, with a threshold of 0.70 or higher considered acceptable as per Nunnally (1978). Corrected item-total correlations were examined to determine whether the removal of any item would enhance internal consistency.

Exploratory Factor Analysis (EFA) was then conducted to ensure the constructs were clearly defined and distinct from one another. The Kaiser-Meyer-Olkin (KMO) measure was assessed, with values above 0.60 deemed adequate. Bartlett's Test of Sphericity was used to verify sufficient inter-item correlations for factor analysis. Principal Component Analysis with Varimax rotation was applied to confirm that items loaded appropriately onto their respective constructs, with factor loadings greater than 0.50 considered significant.

3.4.3 Descriptive Statistical Analysis

Descriptive statistics were calculated to provide an overview of central tendency and dispersion for each construct. Mean scores were used to indicate the maturity level of each cybersecurity domain, while standard deviations reflected the variability across participating mining organizations (Pallant, 2020). Maturity levels were categorized using specific cut-offs means below 2.5 indicated low maturity, values between 2.5 and 3.5 indicated moderate maturity, and

values above 3.5 signified high maturity. This approach facilitated an assessment of the preparedness and governance status within the sector.

3.4.4 Correlation Analysis

Pearson's correlation coefficients were computed to examine the relationships between each independent variable and incident exposure. The strength of associations was interpreted as follows: 0.10–0.29 indicated a weak relationship, 0.30–0.49 a moderate relationship, and 0.50 or above a strong relationship. Statistical significance was assessed at both $p < 0.05$ and $p < 0.01$. This analysis provided preliminary insight into expected relationships and aided in identifying potential multicollinearity prior to regression analysis.

3.4.5 Multiple Regression Analysis

Multiple linear regression was employed to assess the predictive power of cybersecurity control domains on incident exposure.

3.4.5.1 Model Specification

Incident Exposure was treated as the dependent variable. The independent variables included:

X1 = Ransomware Preparedness

X2 = Insider Threat Mitigation

X3 = Technology Controls

X4 = Security Awareness

X5 = Governance Maturity

The regression model was specified as:

$$Y = \beta0 + \beta1X1 + \beta2X2 + \beta3X3 + \beta4X4 + \beta5X5 + \varepsilon$$

In this model, β0 is the constant term (intercept), β1 to β5 are the coefficients for the predictor variables, and ε represents the random error. Standardised beta values were used to compare the relative influence of each predictor in the model. Model explanatory power was summarised using R^2, while Adjusted R^2 was reported to account for the number of predictors included. Individual predictors were tested using t-statistics, and the overall model fit was evaluated using the F-test.

3.4.6 Assumption Testing for Regression

All standard regression assumptions were tested to ensure the validity of the results. Linearity was assessed by plotting predicted versus observed values and inspecting residual plots for straight-line relationships. Independence of errors was evaluated using the Durbin–Watson statistic, with values between 1.5 and 2.5 regarded as acceptable. Homoscedasticity was checked through standardized residual plots, where a random scatter pattern indicated constant error variance. Multicollinearity was examined using Variance Inflation Factor (VIF) and tolerance values, with VIFs below 10 and tolerance above 0.10 considered satisfactory. Normality of residuals was assessed by reviewing histograms and P-P plots of the standardized residuals.

3.4.7 Moderation and Mediation Testing

To examine how social and technological factors interact, both moderation and mediation analyses were conducted. The moderation analysis tested whether governance maturity alters the relationship between technological controls and incident exposure. Predictor variables were mean-centred, interaction terms were created by multiplying the centred predictors by governance maturity scores, and the resulting interaction effects were assessed.

For mediation, the analysis evaluated whether security awareness helps explain the relationship between insider threat mitigation and incident exposure. The procedure followed the steps outlined by Baron and Kenny (1986), and bootstrapping was applied to estimate the indirect effects.

Together, these analyses provided deeper support for the theoretical model by clarifying whether stronger governance strengthens the effectiveness of technological safeguards in reducing incident exposure or whether the expected reinforcing effect is not observed.

3.4.8 Robustness Checks

To verify the stability of the results, the regression models were re-estimated after excluding potential outliers. Additional model specifications were also tested to assess whether the key predictors remained statistically and substantively meaningful. These checks suggested that the findings were robust and were not driven by a small number of atypical cases or by a single modelling choice.

3.4.9 Analytical Workflow Model

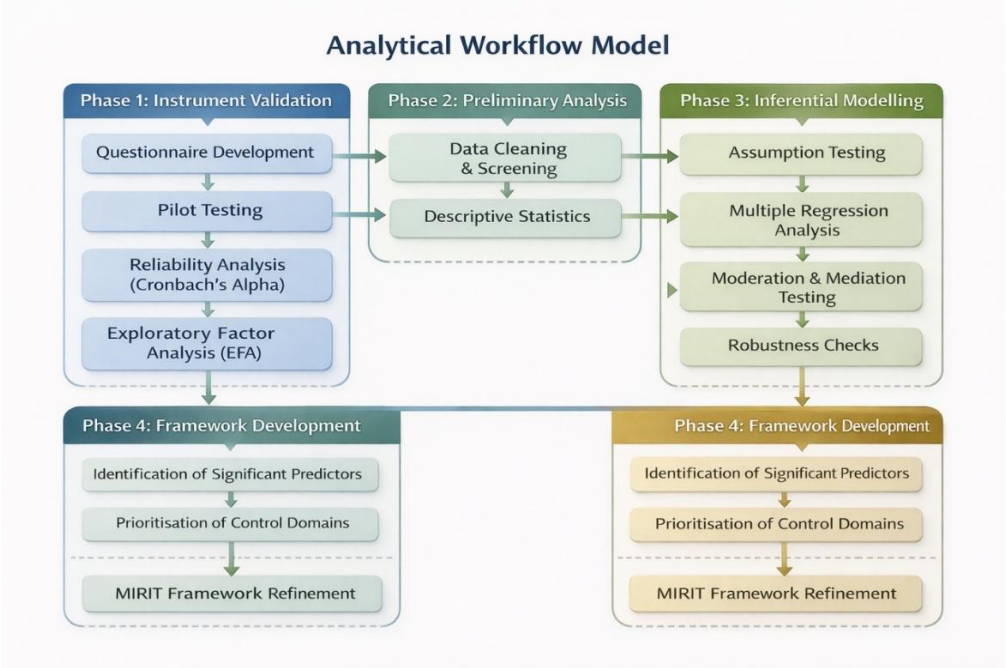

Figure 3.2: Analytical Workflow Model

3.5 Ethical Considerations

Ethical considerations were prioritised throughout the study. Participation was voluntary, and prospective participants were provided with sufficient information about the purpose and procedures of the research before taking part. No personal identifiers were collected, and all organisational information was anonymised to protect confidentiality.

Electronic informed consent was obtained prior to the start of the survey. All data were stored securely with access restricted to the researcher. Findings were reported only in aggregated form, ensuring that no individual organisation could be identified from the results.

In summary, the study followed institutional standards for confidentiality, data security, and responsible research procedures.

3.6 Conclusion

All this laid out the methods behind building the MIRIT Framework. A quantitative, cross-sectional approach was used, based on positivist philosophy to test how different cybersecurity controls relate to incident exposure in Zimbabwe's mining sector. Purposive sampling made sure participants were informed, and the structured surveys turned complex ideas into clear, measurable variables.

By analysing the data through descriptive stats, reliability checks, correlation, and regression, a solid foundation for the framework was built. The careful approach means the MIRIT Framework stands on real evidence, strong theory, and fits the real-world context of Zimbabwe's mining industry. The next section presents the results generated from this analytical process.

CHAPTER 4: Data Analysis and Findings

4.1 Introduction

Chapter 4 reports the survey results from Zimbabwe's mining sector and evaluates the current state of cybersecurity practice across participating organisations. Specifically, it reviews ransomware preparedness, insider-threat mitigation approaches, existing technical controls, security awareness levels, and the maturity of governance structures. The chapter then brings these elements together to explain how they relate to organisations' exposure to cyber incidents.

The chapter is organised as follows. It begins by reporting the response rate and describing the profile of survey respondents. It then presents the reliability analysis to assess whether the survey scales measured the intended constructs consistently. Next, descriptive statistics are used to summarise the maturity levels across the main cybersecurity domains. The analysis then moves to relationships between the study variables and cyber incident exposure, using correlation analysis and multiple regression. The chapter concludes by summarising the key statistical results and linking them back to the study's research questions.

All the number crunching happened in SPSS, with significance set at the 0.05 and 0.01 levels.

4.2 Presentation of Data

4.2.1 Response Rate

The team sent out 95 electronic questionnaires to professionals in Zimbabwe's mining sector. Out of those, 78 people responded. After checking for complete and consistent answers, 72 surveys made the final cut. That is a usable response rate of 75.8%.

Having 72 completed surveys meets the minimum needed for running multiple regression analysis with five predictor variables.

4.2.2 Demographic Characteristics of Respondents

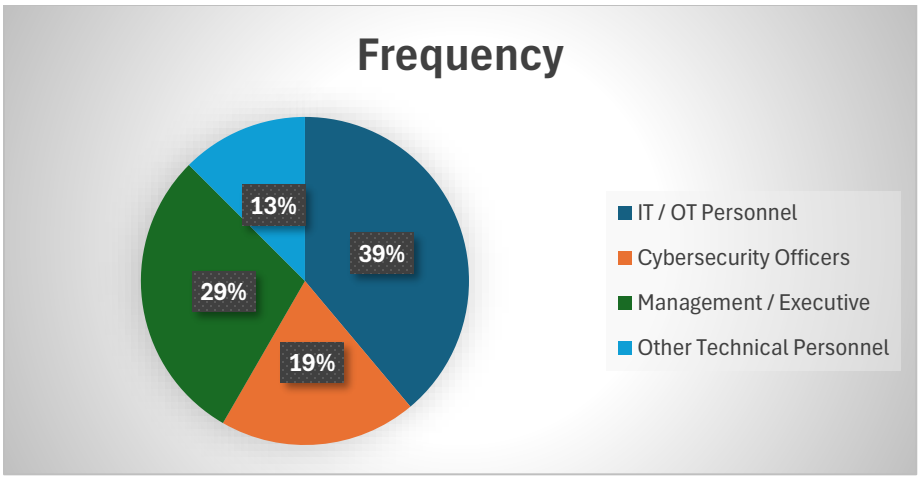

Figure 4.1: Distribution of Respondents by Role (N = 72)

The largest proportion of respondents consisted of IT/OT personnel (38.9%), followed by management-level participants (29.2%). Cybersecurity officers accounted for 19.4% of the sample.

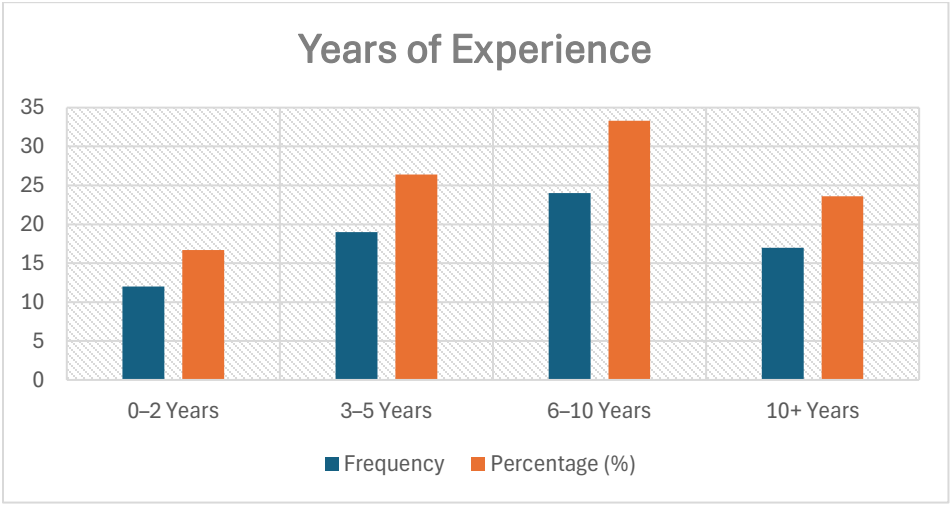

Figure 4.2: Years of Experience (N = 72)

The majority of respondents (56.9%) reported more than five years of experience within their organisations.

4.2.3 Reliability Analysis

Internal consistency reliability was assessed using Cronbach's alpha for each multi-item construct.

Construct	Number of Items	Cronbach's Alpha
Ransomware Preparedness	4	0.82
Insider Threat Mitigation	4	0.79
Technological Control Maturity	4	0.85
Security Awareness	4	0.76
Governance Maturity	4	0.74
Incident Exposure	4	0.81

Table 4.3: Reliability Statistics

All constructs exceeded the acceptable reliability threshold of 0.70, indicating satisfactory internal consistency.

4.2.4 Descriptive Statistics

Descriptive statistics were computed to summarise the central tendency and dispersion of each study variable.

Construct	Mean	Standard Deviation
Ransomware Preparedness	3.68	0.64
Insider Threat Mitigation	3.21	0.71
Technological Control Maturity	3.84	0.58
Security Awareness	2.89	0.76
Governance Maturity	2.74	0.82
Incident Exposure	3.12	0.69

Table 4.4: Descriptive Statistics of Cybersecurity Domains

Technological Control Maturity recorded the highest mean score (3.84), while Governance Maturity recorded the lowest (2.74).

4.2.5 Correlation Analysis

Pearson's correlation coefficients were computed to examine relationships among study variables.

Variables	1	2	3	4	5	6

1. Ransomware Preparedness	1					
2. Insider Threat Mitigation	.44**	1				
3. Technological Controls	.49**	.43**	1			
4. Security Awareness	.38**	.55**	.46**	1		
5. Governance Maturity	.43**	.52**	.48**	.56**	1	
6. Incident Exposure	-.54**	-.46**	-.47**	-.51**	-.58**	1

Note: p < 0.01

Table 4.5: Pearson Correlation Matrix

All independent variables exhibit statistically significant negative relationships with Incident Exposure.

4.2.6 Multiple Regression Results

Multiple regression analysis was conducted to determine the predictive influence of cybersecurity control domains on Incident Exposure.

Predictor Variable	**Standardised Beta (β)**	**t-value**	**Sig. (p)**
Ransomware Preparedness	-0.27	-3.71	0.000
Insider Threat Mitigation	-0.22	-2.98	0.004
Technological Controls	-0.20	-2.74	0.007
Security Awareness	-0.23	-3.11	0.002
Governance Maturity	-0.31	-4.26	0.000

Table 4.6: Regression Analysis Results

Model Summary:

$R^2 = 0.52$

Adjusted $R^2 = 0.50$

$F = 29.83$

$p < 0.001$

The regression model accounts for 52% of the variance in Incident Exposure.

4.3 Analysis of Findings

This section analyses the statistical results presented in Section 4.2 above. The analysis focuses on hypothesis testing and interpretation of regression coefficients to determine the influence of each cybersecurity control domain on Incident Exposure level.

4.3.1 Overall Model Evaluation

Multiple regression analysis was conducted with Incident Exposure as the dependent variable and five independent variables: Ransomware Preparedness, Insider Threat Mitigation, Technological Controls, Security Awareness, and Governance Maturity.

The regression model was statistically significant:

$F(5, 66) = 29.83, p < 0.001$

The model explains 52% of the variance in Incident Exposure ($R^2 = 0.52$), with an adjusted R^2 of 0.50. This indicates that the combined set of predictors accounts for a substantial proportion of variation in cyber incident exposure among the sampled mining organisations.

All regression assumptions were examined prior to interpretation. Variance Inflation Factor (VIF) values were below the accepted threshold of 10, indicating absence of multicollinearity. Residual plots confirmed homoscedasticity and linearity, and the Durbin–Watson statistic was within acceptable range, indicating independence of errors.

4.3.2 Hypothesis Testing

Hypothesis 1

H1: Ransomware preparedness is negatively associated with incident exposure.

Ransomware preparedness demonstrated a statistically significant negative relationship with incident exposure ($\beta = -0.27$, $t = -3.71$, $p < 0.001$).

This indicates that higher levels of ransomware preparedness are associated with lower levels of reported incident exposure.

Decision: Hypothesis 1 is supported.

Hypothesis 2

H2: Insider threat mitigation is negatively associated with incident exposure.

Insider threat mitigation showed a statistically significant negative relationship with incident exposure ($\beta = -0.22$, $t = -2.98$, $p = 0.004$).

This suggests that stronger insider monitoring, access governance, and mitigation practices correspond with reduced exposure to cyber incidents.

Decision: Hypothesis 2 is supported.

Hypothesis 3

H3: Technological control maturity is negatively associated with incident exposure.

Technological controls demonstrated a statistically significant negative association with incident exposure ($\beta = -0.20$, $t = -2.74$, $p = 0.007$).

This result indicates that improved implementation of technological safeguards such as multi-factor authentication, segmentation, and patch management contributes to reduced cyber incident exposure.

Decision: Hypothesis 3 is supported.

Hypothesis 4

H4: Security awareness is negatively associated with incident exposure.

Security awareness was found to have a statistically significant negative relationship with incident exposure ($\beta = -0.23$, $t = -3.11$, $p = 0.002$).

This suggests that increased cybersecurity awareness and training among employees is associated with lower incident exposure levels.

Decision: Hypothesis 4 is supported.

Hypothesis 5

H5: Governance maturity is negatively associated with incident exposure.

Governance maturity emerged as the strongest predictor of incident exposure ($\beta = -0.31$, $t = -4.26$, $p < 0.001$).

This indicates that higher levels of structured governance, policy enforcement, and executive oversight are associated with significantly reduced cyber incidents.

Decision: Hypothesis 5 is supported.

4.3.3 Relative Strength of Predictors

Based on standardised beta coefficients, the predictors rank in descending order of influence as follows:

1. Governance Maturity (β = -0.31)
2. Ransomware Preparedness (β = -0.27)
3. Security Awareness (β = -0.23)
4. Insider Threat Mitigation (β = -0.22)
5. Technological Controls (β = -0.20)

Governance maturity demonstrates the largest absolute beta coefficient, indicating the strongest relative influence in reducing incident exposure within the regression model.

4.3.4 Summary of Hypothesis Testing

Hypothesis	Statement	Result
H1	Ransomware preparedness negatively affects incident exposure	Supported
H2	Insider threat mitigation negatively affects incident exposure	Supported
H3	Technological controls negatively affect incident exposure	Supported
H4	Security awareness negatively affects incident exposure	Supported
H5	Governance maturity negatively affects incident exposure	Supported

Table 4.7: Summary of Hypothesis Testing Results

All five hypotheses were supported at statistically significant levels.

4.4 Discussion of Results

The regression analysis shows that all five independent variables strongly predict Incident Exposure. Together, these cybersecurity control domains account for 52% of the variation in cyber risk outcomes across the mining organisations studied. That is a pretty significant chunk, meaning the chosen areas clearly matter when it comes to reducing cyber incidents.

Among the five, governance maturity stands out. It has the largest impact, with a standardised beta of -0.31. So, when mining organisations improve their governance structures, they see the biggest drop in incident exposure compared to changes in the other domains. This is not just a fluke in the numbers, governance consistently comes out as the top factor in both the correlation and regression analyses, always showing a strong negative link to incident exposure.

Ransomware preparedness comes next, with a beta of -0.27. The data suggests that when organisations have solid plans for responding to ransomware, keep up with backup management, and use network segmentation, they see fewer incidents. The results back up what the descriptive stats show, organisations prepared for ransomware generally report lower exposure.

Security awareness ($\beta = -0.23$) and insider threat mitigation ($\beta = -0.22$) both play meaningful roles, too. Their effects are close in size, showing that both regular training and active insider threat monitoring make a difference in cutting down cyber incidents. While insider threat mitigation has a slightly smaller effect than governance or ransomware preparedness, it still matters a lot in the bigger picture.

Technological control maturity recorded the smallest standardised beta ($\beta = -0.20$), although the effect remained statistically significant. This suggests that technical safeguards contribute to reducing incident exposure, but their influence is weaker than that of governance and behavioural factors in this study. All five beta coefficients are negative, which means higher maturity in any domain leads to less incident exposure.

Looking at the whole pattern, cybersecurity resilience in these mining organisations depends on several connected areas. Governance, preparedness, awareness, insider mitigation, and technological controls all help explain the differences in how much organisations get hit by cyber incidents.

4.5 Comparison with Literature

What is interesting is how much these findings line up with past research. The big impact of governance maturity matches what other studies have found, strong leadership and structured governance go a long way in cutting cyber risks (Safitra et al., 2023; Maphosa, 2024). Those earlier studies also highlight how central governance is for bringing all the other cybersecurity controls together.

The clear link between ransomware preparedness and lower incident exposure fits what Lawall and Beenken, (2024) reported as well, they found that having structured response plans and strict control over privileged accounts really helps defend against ransomware. The results here show the same thing in the mining sector.

Insider threat mitigation also stands out, echoing research that focuses on access governance and monitoring people's behaviour to stop insider risks (Clifton, 2024; Alsowail and Al-Shehari, 2022). Those studies stress the need for structured frameworks to handle insider threats, which matches What is seen in these results.

Security alertness agrees with a broader position in the literature that recognises human behaviour as a central component of cybersecurity (Saeed et al., 2023). The result is to support that view: organisations with stronger security awareness programmes reported lower levels of incident exposure.

Although technological controls showed a comparatively smaller effect than the other factors, their contribution remained statistically significant. This finding is consistent with the defence-in-depth perspective, which emphasises that technical safeguards are necessary but most effective when reinforced by strong governance and secure behavioural practices (Kaur et al., 2023).

Altogether, the findings are broadly consistent with established research, particularly the emphasis placed on governance and the human element in managing cyber risk.

CHAPTER 5: Discussion and Recommendations

5.1 Introduction

5.2 Structure of the Chapter

This chapter discusses the findings presented in Chapter 4 to understand how ransomware and insider threats affect mining organisations in Zimbabwe. The discussion is organised around the research questions guiding the study. Each section looks at the findings related to a specific research question and interprets the findings within the context of cybersecurity risk management.

This also discusses the implications of the findings for the development of a cybersecurity framework designed to mitigate ransomware and insider threats in Zimbabwe's mining sector. The discussion draws on international cybersecurity principles such as those promoted by the National Institute of Standards and Technology, while also taking into account the operational realities faced by mining operations in Zimbabwe. Through this analysis, the chapter provides a foundation for strengthening cybersecurity resilience in the mining industry.

5.3 Nature of ransomware and insider threats affecting mining organisations

5.3.1 Ransomware Threats in the Mining Sector

The findings presented in the previous chapter indicate that ransomware attacks are now being recognised as a emerging cybersecurity threat within the mining industry. Participants in this study responded that ransomware incidents have affected organisations within the sector either directly or indirectly. In many cases, respondents indicated that ransomware attacks usually originate through phishing emails, opening of malicious attachments, or compromised user credentials. These methods enable attackers to gain initial access to organisational systems before deploying ransomware that encrypts critical organisational data.

These findings agree with global cybersecurity trends showing that ransomware attacks in many cases rely on social engineering techniques to infiltrate organisational networks. Phishing campaigns remain one of the most common method used by cybercriminals because they exploit common human behaviour rather than just looking for technical vulnerabilities.

5.3.2 Insider Threats within Mining Organisations

Participants in the study indicated that insider incidents often occur through actions such as users sharing login credentials, mishandling sensitive information, or failing to follow established cybersecurity procedures. It is this kind of behaviour that expose organisational systems to cyber threats or exposes critical systems to unauthorised access. Sometimes, insiders with privileged access to organisational networks may also have the ability to bypass certain security controls, increasing the potential impact of insider-related incidents if such accounts are compromised.

5.3.3 Interaction Between External and Insider Threats

The findings of this study also suggest that ransomware and insider threats are not separate categories of cybersecurity risk. They, in many sases, interact in ways that increase the overall vulnerability of mining organisations computer systems. For example, phishing attacks used by ransomware groups frequently target employees in order to obtain login credentials or gain access. Once credentials are compromised, attackers may navigate the network in ways that just like a legitimate user.

Similarly, insiders may unintentionally enable ransomware attacks by failing to identify possible phishing emails or by using weak passwords that can be easily brute-forced by attackers. In this way, human behaviour often acts as a bridge between external cyber threats and internal organisational vulnerabilities. This interaction highlights the importance of addressing both external cyber threats and insider risks within a unified cybersecurity strategy.

Most cybersecurity frameworks are mainly designed with need for layered security controls that address multiple threat vectors simultaneously. Risk management guidelines developed by the National Institute of Standards and Technology stress the importance of combining technical safeguards with organisational IT governance measures such as access control, monitoring, and incident response capabilities. Applying these principles within mining environments may help organisations detect suspicious behaviour in time and avoid successful cyberattacks.

5.3.4 Implications for Cybersecurity Risk Management in Mining

The findings of the first research question indicate that ransomware and insider threats are two of the most significant cybersecurity challenges facing mining organisations in Zimbabwe. While ransomware attacks exploit weaknesses in user awareness and network access controls, insider threats arise from inadequate access management and insufficient monitoring of user activity. Both types of threats show how cyber incidents usually happen when there is interaction between technological vulnerabilities and human behaviour within organisational IT environments.

From a risk management angle, the findings of this study highlight the importance of strengthening both technical and organisational cybersecurity measures within the mining sector. Mining organisations must not just implement effective technical safeguards such as network monitoring and malware protection systems, but also strengthen governance practices especially staff awareness training, access management policies, and proper incident response planning.

Addressing these issues is critical for reducing the likelihood and impact of cyber incidents within mining operations. Improving user awareness of ransomware and insider threats, help mining organisations to take proactive steps well in time to strengthen cybersecurity preparedness and protect critical systems from being disrupted.

5.4 Cybersecurity Vulnerabilities in Mining Infrastructure

5.4.1 Legacy Systems and Operational Technology Vulnerabilities

One of the major issues identified in the findings is the continued use of legacy operational technology (OT) systems within mining environments. Many mining operations depend on industrial control systems, supervisory control and data acquisition (SCADA) systems, and other automated control technologies that were originally designed to without security in mind. They were rather designed for efficiency. As a result, such systems may lack modern security features such as strong authentication mechanisms, encryption protocols, and advanced intrusion detection capabilities.

The findings from this research indicate that these legacy systems has a potential to create significant vulnerabilities because they are sometimes integrated with modern information technology (IT) networks in order to support remote monitoring and operational management. While this integration improves operational visibility and productivity, it also introduces additional

possible attack surface area that may be utilised by cybercriminals. Attackers who gain access to corporate IT networks may be able to move laterally in the network if adequate segmentation between IT and OT systems is not done.

5.4.2 Weak Access Control and Identity Management

Another vulnerability identified in the findings relates to weaknesses in access control mechanisms implemented by mining organisations. Participants reported that in some cases employees and contractors will have access rights that is more than their operational requirements. Such situations increase the risk of both accidental and intentional misuse of organisational systems. If users have excessive rights, they may have the ability to access sensitive organisational data or modify critical system configurations thereby creating room for external attacks.

Weak password management practices were also identified as a potential vulnerability within some mining organisations surveyed. Use of passwords that are not complex enough, passwords not frequently beings changed, or shared login credentials may create opportunities for attackers to gain unauthorised access to organisational systems. Once access is obtained, attackers may escalate privileges and move across networks to search for exploitable data or operational systems that can be used in ransomware attacks.

5.4.3 Limited Monitoring and Detection Capabilities

The findings also highlighted that many mining organisations have limited capabilities for monitoring network activity and detecting cyber incidents in real time. While some organisations have implemented basic security tools like antivirus software and firewalls, more advanced monitoring tools such as security information and event management (SIEM) systems or behavioural analytics platforms are not widely used. Without these tools, effective monitoring of suspicious activities within organisational networks may remain undetected for extended periods of time.

Limited monitoring capabilities can increase the impact of cyber incidents. Attackers who gain access to organisational networks may remain undetected while conducting reconnaissance, escalating privileges, and deploying malicious software. In ransomware attacks, this period of

undetected activity, allows attackers to identify critical systems and data before launching encryption attacks. To reduce this risk, mining organisations need to implement continuous monitoring systems that are able to detect unusual network behaviour and suspicious user activity and notify administrators of the systems in real time.

5.4.4 Implications for Mining Sector Cybersecurity

The vulnerabilities identified in this study highlight several cybersecurity challenges currently present in Zimbabwe's mining sector. Legacy operational systems, weak identity management practices, and limited network monitoring mechanisms all create an environment in which cyber threats such as ransomware and insider attacks can occur more easily. These vulnerabilities are not unique to Zimbabwe but are commonly observed in industrial environments undergoing digital transformation.

However, the presence of such vulnerabilities also indicates that there is a real need for improving cybersecurity resilience within the mining sector. Addressing the current issues requires an integration of technological and organisational measures. From a technical point of view, mining organisations should consider and prioritise network segmentation between IT and OT environments, implement stronger authentication mechanisms, and deploy advanced monitoring tools capable of detecting suspicious activity across IT/OT network systems.

From an organisational perspective, improved cybersecurity governance and staff awareness programmes are all important. Employees and contractors should be made to understand the cybersecurity risks associated with their daily activities and adhere to established security operational procedures. By strengthening both technical controls and organisational practices, mining organisations can significantly reduce the vulnerabilities that enable ransomware and insider threats to occur.

5.5 Effectiveness of Existing Cybersecurity Controls in Mining Organisations

5.5.1 Organisational Cybersecurity Policies and Governance

This research found out that many mining organisations have established formal cybersecurity policies designed to guide the protection of organisational information systems. These policies

typically outline acceptable use of organisational IT resources, password management requirements, data protection guidelines, and procedures for responding to cybersecurity incidents. The presence of such policies suggests that mining organisations recognise the importance of cybersecurity governance and have taken initial steps to formalise security practices.

However, the results also suggest that the existence of policies does not always translate to their religious implementation. In some organisations, cybersecurity policies are not consistently enforced or regularly updated to the prevailing regional cyber environment. Employees, in some case, have limited awareness of the specific requirements detailed in these policies, particularly where training and awareness programmes are not conducted regularly. As a result, organisational policies may exist primarily as compliance documents rather than fully implemented to guide cybersecurity behaviour.

Cybersecurity governance research emphasises that policies must be supported by effective implementation mechanisms in order to have an impact on organisational behaviour. This includes regular policy reviews, clear role assignment of security responsibilities, and consistent enforcement of security measures across the organisation. Technology adoption studies have also shown that organisational commitment and user acceptance significantly influence the effectiveness of cybersecurity practices (Masimba & Zuva, 2021). Without strong governance structures and leadership support, cybersecurity policies may fail to translate into effective tools to guard against cyber attacks.

5.5.2 Technical Security Controls and System Protection

The findings also established that mining organisations rely on several technical safeguards to protect their information systems from cyber threats. Commonly implemented controls include firewalls, antivirus software, network access restrictions, and system patching. These controls represent important cybersecurity practices designed to prevent unauthorised access and protect organisational data from common malware threats.

While these measures provide an important baseline level of protection, the study results suggest that they may not always be sufficient to defend against more sophisticated cyber threats such as advanced ransomware attacks. Modern ransomware campaigns often use sophisticated attack

techniques that involve phishing, credential theft, lateral movement, and privilege escalation before deploying the actual ransomware payloads. Basic technical controls alone may therefore struggle to detect such attacks at early stages before it is too late.

5.5.3 Employee Awareness and Cybersecurity Culture

Another important aspect of cybersecurity effectiveness is employee awareness and organisational security culture change. The findings from Chapter 4 indicate that many mining operations have introduced various forms of cybersecurity awareness initiatives, that include staff training sessions and awareness campaigns designed to educate employees about common cyber risks. These initiatives are designed to reduce human error and improve employee understanding of cybersecurity responsibilities.

Despite these efforts, the results suggest awareness campaigns are not always conducted consistently across all employees of an organisation. In some cases, cybersecurity training may only target IT personnel while other operational staff members receive limited to no structured cybersecurity education. This gap is significant because employees working in operational roles may interact frequently with organisational systems and may therefore be exposed to cyber threats such as phishing emails or malicious links and weakens the whole chain.

5.5.4 Backup and Incident Response Preparedness

The findings also highlight variations in how mining organisations prepare themselves for cybersecurity incidents such as ransomware attacks. Several organisations do data backups, but the frequency and testing of these backup systems vary considerably. In some cases, backups are conducted regularly but restoration procedures are not regularly tested. Without periodic testing, organisations may not be certain whether backup systems can successfully restore operations following a ransomware incident or not.

Incident response planning also appears to vary among mining organisations. Some reported having laid down procedures for responding to cyber incidents, while others rely on informal processes or support from external IT service providers. The absence of clearly defined incident

response strategies may delay organisational response during cybersecurity incidents, increasing the potential impact should any incident occur.

5.5.5 Implications for Cybersecurity Effectiveness in Mining

To sum it up, the findings addressing the third research question indicate that mining organisations have implemented several basic cybersecurity practices but continue to face challenges in achieving complete protection against modern cyber threats. Security policies, technical safeguards, and awareness programmes provide an important starting point for cybersecurity management but weaknesses in policy enforcement, limited advanced monitoring capabilities, and inconsistent training initiatives reduce the overall effectiveness of these measures.

These findings suggest that mining organisations must adopt a more integrated cybersecurity strategy that combines governance, technical protection, and human-centred security practices. Strengthening cybersecurity governance structures, improving employee awareness programmes, and implementing advanced threat detection capabilities would significantly improve the resilience of mining organisations against ransomware and insider threats.

5.6 Requirements for an Effective Cybersecurity Framework for the Mining Sector

The fourth research question tried to identify the requirements for an effective cybersecurity framework capable of mitigating ransomware and insider threats within Zimbabwe's mining sector. The previous sections of this chapter examined the nature of the threats affecting mining organisations, the vulnerabilities that enable these threats, and the effectiveness of existing cybersecurity practices. Building on these findings, this section discusses the key organisational and technical elements that should form the foundation of the proposed cybersecurity framework tailored to the mining environment.

5.6.1 Improving Identity and Access Management

The findings from the previous sections show weaknesses in access control practices as one of the major vulnerabilities affecting mining organisations. Incorrect user privileges, weak password practices, and the absence of strong authentication mechanisms in place increase the likelihood of both insider misuse and external cyber intrusion. Addressing these issues requires the

implementation of robust identity and access management methods that ensure users only have enough privileges to access systems and data necessary for their roles.

An effective cybersecurity framework for the mining sector should therefore implement the principle of least privilege, where access rights are restricted according to operational responsibilities. This approach reduces the risk that compromised credentials or malicious insiders can access sensitive areas of IT systems. In addition, the implementation of multi-factor authentication can reduce the risk of unauthorised access by requiring additional verification beyond traditional password-based authentication.

Identity and access management practices are widely accepted as a core component of organisational cybersecurity governance. International cybersecurity standards such as those promoted by the National Institute of Standards and Technology emphasise identity management as an important security function that supports the protection of critical systems. For mining organisations operating in digitally connected environments, strengthening identity and access management is so important for mitigating both external cyber threats and insider-related risks.

5.6.2 Network Segmentation and Protection of Operational Technology

Another important requirement identified through the findings relates to the protection of operational technology (OT) systems used in mining environments. As discussed earlier, mining operations rely heavily on industrial control systems and other automated technologies that support production processes. The integration of these systems with corporate IT networks introduces cybersecurity risks if adequate network segmentation is not implemented.

An effective cybersecurity framework should therefore be designed with separation of IT and OT networks in order to reduce the likelihood for attackers to move laterally across organisational systems. Network segmentation limits the spread of cyber intrusions by isolating critical operational systems from external networks and less sensitive organisational systems. If attackers gain access to a corporate IT network, proper segmentation can prevent them from directly accessing industrial control systems responsible for critical mining operations.

5.6.3 Continuous Monitoring and Threat Detection

The findings presented in the previous chapter also revealed that limited monitoring capabilities bring with it significant weakness within many mining organisations. Without effective monitoring systems, cyber intrusions may remain undetected for long periods of time, allowing attackers to escalate privileges, move laterally across networks, and introduce ransomware without immediate detection.

A cybersecurity framework designed for the mining sector should therefore give priority to the implementation of continuous monitoring and threat detection mechanisms. These mechanisms may include security information and event management systems, intrusion detection systems, and behavioural monitoring tools capable of identifying suspicious user activities or unusual network behaviour. Continuous monitoring enables organisations to detect cyber incidents at early stages and initiate appropriate response actions before attacks cause widespread disruption.

Threat intelligence research has shown that modern cyberattacks often involve multiple stages, including reconnaissance, credential compromise, lateral movement, and data exfiltration. Frameworks such as those developed by the MITRE Corporation illustrate how cyber attackers exploit different system weaknesses during each stage of an attack. Implementing monitoring systems capable of detecting these activities is essential for improving organisational cybersecurity resilience.

5.6.4 Employee Awareness and Insider Threat Management

Human factors are a major consideration in many cybersecurity incidents, especially those involving phishing attacks and credential compromise. The findings from the study indicate that employee behaviour can significantly influence the effectiveness of cybersecurity practices within mining organisations. As a result, any cybersecurity framework designed for the sector must incorporate strategies for improving employee awareness and managing insider risk.

Regular cybersecurity awareness training programmes should be implemented to educate employees about common cyber threats, safe system usage practices, and organisational security policies. Such programmes should not be limited to IT personnel but should include operational staff, contractors, and management personnel who interact with organisational systems. Phishing

simulation exercises and regular security briefings can further reinforce cybersecurity awareness and help employees recognise potential threats.

In addition to awareness training, organisations should implement insider threat monitoring systems that can track unusual user behaviour and identify potential security risks. These strategies may involve analysing patterns of system access, monitoring unusual data transfers, or identifying unauthorised attempts to access sensitive systems and any other unusual network activities. Research on insider threat detection highlights the importance of combining behavioural monitoring with organisational policies and risk assessment mechanisms to effectively identify potential insider risks (Clifton, 2024).

5.6.5 Incident Response and Cyber Resilience

Another key requirement identified through the findings is the need for improved incident response capabilities within mining organisations. Cybersecurity incidents such as ransomware attacks require immediate and organised responses to minimise operational disruption and financial losses. Without clearly defined incident response procedures, organisations may struggle to contain cyber incidents effectively.

A cybersecurity framework for the mining sector should therefore include establishment of formal incident response plans that define procedures for detecting, reporting, and responding to cybersecurity incidents. These plans should clearly outline roles and responsibilities for incident response teams, communication procedures during cyber incidents, and recovery strategies for systems restoration after an incident. Regular testing of incident response plans through simulation exercises can help mining organisations to evaluate their readiness to respond to cyber incidents.

Cyber resilience strategies emphasise the importance of maintaining reliable data backups and recovery mechanisms that enable organisations to restore operations following cyber incidents. In the context of ransomware attacks, having secure and regularly tested backup systems is particularly important because it allows organisations to recover encrypted data without paying ransom demands.

5.6.6 Implications for Framework Development

The findings addressing the fourth research question highlight several important components that should be included in a contextualised cybersecurity framework for Zimbabwe's mining sector. These components include robust identity and access management mechanisms, network segmentation between IT and OT systems, continuous monitoring capabilities, employee awareness programmes, and well-defined incident response strategies.

Integrating these elements into a comprehensive cybersecurity framework would enable mining organisations to address both technological and organisational aspects of cybersecurity risk. Such a framework should also remain adaptable to always changing cyber threats and technological developments within the mining industry.

Overall, the findings suggest that effective cybersecurity protection in mining environments requires a layered defence strategy that combines governance, technical safeguards, and human-centred security practices. By implementing a structured cybersecurity framework incorporating these elements, mining organisations can significantly improve their ability to prevent, detect, and respond to ransomware and insider threats.

5.6.7 Proposed Cybersecurity Framework for the Mining Sector

Based on the findings of this study and the cybersecurity requirements identified in the preceding sections, a contextualized cybersecurity framework is proposed to mitigate ransomware and insider threats within Zimbabwe's mining sector. The framework integrates governance, technological safeguards, and human-centred security practices in order to strengthen organisational cyber resilience.

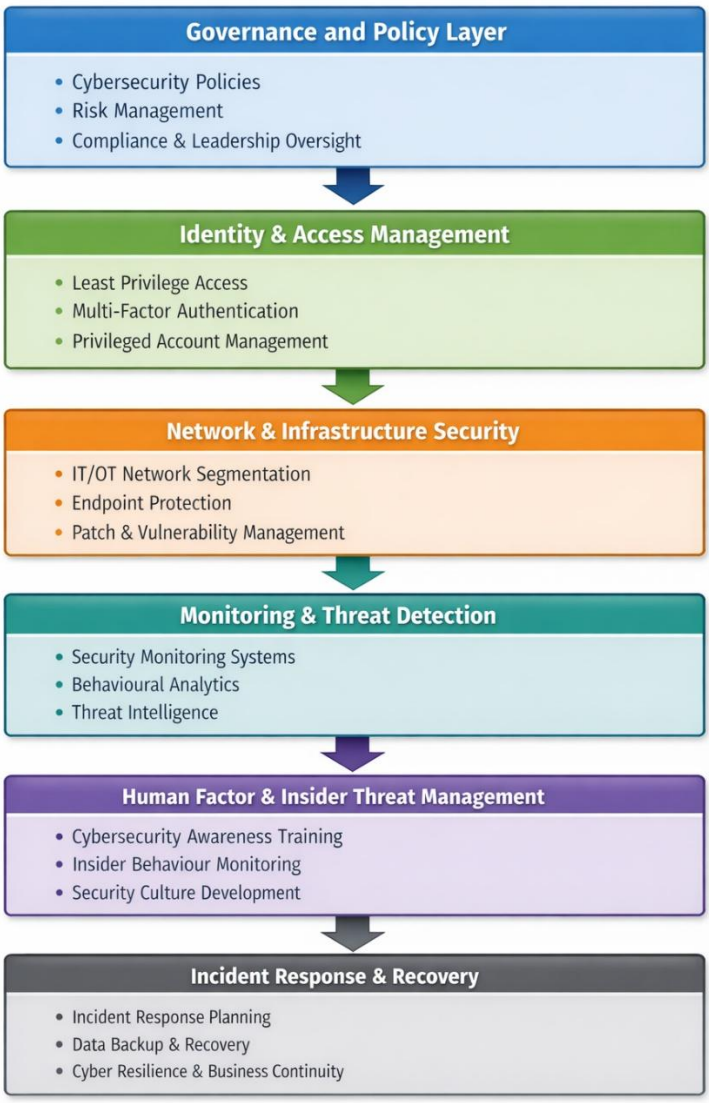

Figure 5.1: Proposed Cybersecurity Framework for *Mitigating Ransomware and Insider Threats in Zimbabwe's Mining Sector*

5.7 Overview of the Framework

The proposed cybersecurity framework presented in Figure 5.1 was developed based on the empirical findings of this study and the cybersecurity challenges identified within Zimbabwe's mining sector. The framework integrates organisational governance mechanisms, technical security controls, and human-centred security practices in order to mitigate ransomware and insider threats. The framework is built upon a layered defence approach in which different security components work together to prevent, detect, and respond to cyber incidents.

This framework addresses the vulnerabilities identified in the study, including observed weak access control practices, limited monitoring capabilities, and the growing exposure of mining organisations to ransomware attacks. The framework also aligns with widely recognised cybersecurity risk management principles such as those promoted by the National Institute of Standards and Technology, which emphasise governance, detection capabilities, and organisational resilience as core components of effective cybersecurity strategies.

5.7.1 Governance and Policy Layer

The foundation of the framework is the governance and policy layer, which establishes the organisational structures required to support effective cybersecurity management. Effective cybersecurity governance requires clear policies that define acceptable system access, security responsibilities, and incident response procedures. Leadership oversight and risk management processes ensure that cybersecurity requirements are integrated into organisational decision-making and operational planning.

Within mining organisations, strong governance structures are particularly important because cybersecurity risks affect both information systems and operational technology environments. Governance mechanisms help ensure that cybersecurity practices are implemented consistently across the organisation and that security responsibilities are clearly defined.

5.7.2 Identity and Access Management

The second layer focuses on identity and access management. The findings of the study indicated that weak access control practices represent a major vulnerability within mining organisations. The framework therefore emphasises the implementation of the principle of least privilege in access controls, ensuring that employees only have access to the systems necessary for their operational roles, not anything more.

Multi-factor authentication and privileged account management further strengthen identity protection by reducing the likelihood of unauthorised system access. These measures are necessary for mitigating ransomware attacks, which mainly rely on compromised credentials to gain access to organisational networks.

5.7.3 Network and Infrastructure Security

The third layer addresses the protection of organisational infrastructure, including both information technology and operational technology systems. Mining environments usually rely on industrial control systems and automated equipment connected to corporate networks. Without adequate protection, attackers may exploit these connections to move laterally across systems.

Network segmentation between IT and OT environments therefore forms a key component of the framework. Segmentation limits the spread of cyber intrusions by separating operational systems from corporate networks and external internet access. Additional measures such as endpoint protection and vulnerability management further reduce the likelihood of successful cyber intrusions.

5.7.4 Monitoring and Threat Detection

Continuous monitoring and threat detection represent another critical component of the framework. The findings of the study indicated that limited monitoring capabilities can allow attackers to remain undetected within organisational networks for longer periods of time. Implementing security monitoring tools and behavioural analytics systems enables organisations to identify suspicious activities in time and potential cyber incidents at early stages.

Threat intelligence mechanisms further support monitoring efforts by providing information about emerging cyber threats and attack techniques. By integrating monitoring and threat intelligence capabilities, mining organisations can improve their ability to detect ransomware attacks or insider-related vulnerabilities before they cause any damage to the organisation’s systems.

5.7.5 Human Factor and Insider Threat Management

Human behaviour plays a central role in many cybersecurity incidents. Phishing attacks, credential misuse, and negligent system practices often provide attackers with access into organisational networks. The framework therefore incorporates a dedicated layer addressing employee awareness and insider threat management.

Regular cybersecurity training programmes gives employees the ability to recognise common cyber threats and understand their security responsibilities. Behavioural monitoring systems can also help detect unusual user activity that may indicate insider misuse of organisational systems. Strengthening cybersecurity culture across the organisation encourages employees to follow secure practices and report suspicious activities.

5.7.6 Incident Response and Recovery

The final layer of the framework focuses on incident response and organisational resilience. Even with strong preventative controls, cyber incidents may still occur. Mining organisations must therefore have well-defined procedures for detecting, responding to, and recovering from cyber incidents.

Incident response plans outline the actions required to contain cyber incidents, protect critical systems, and restore operations. Reliable data backup systems and recovery mechanisms are particularly important for mitigating ransomware attacks because they allow organisations to restore encrypted data without paying ransom demands. By combining response planning with recovery capabilities, organisations can maintain operational continuity and minimise the impact of cyber incidents.

5.8 Contribution of the Framework

Overall, the proposed framework provides a structured approach for strengthening cybersecurity resilience within Zimbabwe's mining sector. By integrating governance structures, technical safeguards, monitoring mechanisms, and human-centred security practices, the framework

addresses the key vulnerabilities identified in the study. The layered structure also supports continuous improvement, enabling mining organisations to adapt their cybersecurity strategies as new threats emerge.

The framework therefore provides practical guidance for mining organisations seeking to reduce their exposure to ransomware attacks and insider threats while supporting the secure digital transformation of mining operations.

5.9 Integrated Discussion of Findings

The preceding sections examined the findings of the study in relation to each research question and the development of a contextualised framework. This section integrates those findings in order to identify the general patterns emerging from the data and to explain how these patterns contribute to understanding cybersecurity risks within Zimbabwe's mining sector. By analysing the results presented in the earlier sections, the discussion highlights the relationships between ransomware threats, insider risks, organisational vulnerabilities, and the effectiveness of existing cybersecurity practices.

5.9.1 Convergence of External and Internal Cyber Threats

One of the key insights appearing from the findings is the close relationship between external cyber threats and internal organisational vulnerabilities. The study revealed that ransomware attacks frequently rely on techniques such as phishing and credential compromise, which takes advantage of human behaviour and weak access management practices. At the same time, insider threats arise from abuse of legitimate system access or negligent security practices among employees. Although these threats start from different sources, they often exploit similar weaknesses within organisational IT systems.

This convergence suggests that cyber incidents cannot be understood solely as external attacks or internal misuse of systems. Instead, cyber risks within mining organisations often result from the

nexus between technological vulnerabilities and human behaviour. For example, employees who fail to recognise phishing attempts may unintentionally provide attackers with access credentials, enabling ransomware attacks to be executed from within organisational networks. Similarly, insiders with excessive privileges may create opportunities for unauthorised system manipulation or data compromise if their credentials got in the hands of attackers.

Cybersecurity research increasingly agrees that modern cyber threats usually combine technical exploitation with social engineering tactics. Attackers often target human users as entry points into organisational systems because human behaviour is more difficult to control than technical vulnerabilities. As a result, effective cybersecurity strategies must address both technological and human aspects of security management. An integrated framework is necessary that emphasise integrated security approaches that combine governance, technical safeguards, and user awareness to reduce organisational cyber risk.

5.9.2 Structural Vulnerabilities in Mining Environments

Another important pattern emerging from the findings relates to the operational vulnerabilities present within mining environments. The study identified several technological weaknesses, including reliance on legacy operational technology systems, insufficient or non-existent network segmentation between IT and OT environments, and limited monitoring capabilities. These vulnerabilities increase the potential for cyber threats to compromise both corporate information systems and IT infrastructure.

Industrial sectors such as mining often operate with complex technological infrastructures that include automated equipment, industrial control systems, and remote monitoring technologies. Many of these systems were originally designed to prioritise operational reliability with zero cybersecurity protection mechanisms. As a result, integrating these systems into modern digital environments may introduce security gaps that attackers can exploit and cause a lot of damage.

The findings therefore highlight the need for stronger cybersecurity practices specifically tailored to industrial environments. Measures such as network segmentation, continuous monitoring of

operational systems, and secure remote access controls are very important for protecting industrial infrastructure from cyber threats. Addressing these vulnerabilities is essential for preventing cyber incidents that have the potential to disturb mining operations or compromise sensitive organisational data.

5.9.3 Limitations of Existing Cybersecurity Practices

The findings also reveal that while mining organisations have implemented several cybersecurity measures, the overall effectiveness of these practices remains uneven. Many organisations have established basic security controls such as firewalls, antivirus software, and organisational security policies. However, gaps still remain in areas such as advanced threat detection, consistent policy enforcement, and comprehensive employee awareness programmes.

These gaps highlight an important challenge in cybersecurity management. The presence of security tools and policies does not necessarily guarantee effective protection but cybersecurity effectiveness depends not only on the availability of technical controls but also on how those controls are implemented, monitored, and supported by organisational culture. In environments where policies are poorly enforced or employees lack adequate awareness of cyber hygiene, technical safeguards alone may not prevent cyber incidents.

Research on organisational cybersecurity governance emphasises that effective cybersecurity management requires coordination between technology, processes, and human behaviour for it to be effective. Security policies must be supported by leadership commitment, employee training, and continuous evaluation of security practices. Without such organisational support, cybersecurity initiatives may remain fragmented and fail to address emerging cyber threats effectively as necessary.

5.9.4 Need for a Layered Cybersecurity Strategy

The integrated findings of this study suggest that mining organisations require a comprehensive and layered approach to cybersecurity management. Individual security measures such as firewalls or password policies cannot adequately address the complex cyber threats facing modern organisations. Instead, effective cybersecurity protection requires a coordinated strategy that integrates governance structures, technical security controls, monitoring mechanisms, and human-centred security practices.

The cybersecurity framework proposed here reflects this layered approach. By combining identity and access management, network protection, monitoring capabilities, employee awareness programmes, and incident response mechanisms, the framework addresses multiple aspects of cybersecurity risk simultaneously. Such an approach increases the likelihood that cyber threats will be detected and mitigated before they cause significant operational disruption.

Layered cybersecurity strategies are widely recommended in modern cybersecurity practice because they reduce the likelihood that a single security failure will compromise an entire system. Even if attackers bypass one security control, additional layers of protection may prevent them from achieving their objectives. This principle is particularly important for critical sectors such as mining, where cyber incidents may disrupt essential operational processes.

5.9.5 Implications for Cybersecurity in Zimbabwe's Mining Sector

The findings of this study highlight several important implications for improving cybersecurity resilience within Zimbabwe's mining sector. First, mining organisations must accept that cybersecurity threats are evolving and increasingly targeting industrial environments. As mining operations continue to adopt digital technologies, the potential impact of cyber incidents is likely to increase.

Second, organisations must strengthen cybersecurity governance structures to ensure that security policies and procedures are implemented consistently across operational environments and supported by management. Effective governance helps align cybersecurity initiatives with

organisational objectives and ensures that security responsibilities are clearly defined and followed.

Finally, mining organisations must adopt a proactive approach to cybersecurity that emphasises continuous monitoring, employee awareness, and incident response preparedness. By implementing these measures religiously, organisations can significantly reduce their exposure to ransomware attacks and insider-related security incidents.

In summary, the integrated discussion of findings demonstrates that ransomware and insider threats represent interconnected cybersecurity challenges within Zimbabwe's mining sector. These threats are enabled by a combination of technological vulnerabilities, human factors, and limitations in existing cybersecurity practices. Addressing these challenges requires a coordinated cybersecurity approach that integrates governance, technical safeguards, and organisational awareness.

5.10 Implications for Cybersecurity Management in the Mining Sector

The findings of this study provide several important implications for improving cybersecurity management within Zimbabwe's mining sector. As mining operations continue to adopt digital technologies, the sector is increasingly exposed to cyber threats that can disrupt operations, compromise sensitive data, and create financial and reputational risks for mining organisations. The results of this study highlight the need for mining organisations to adopt more comprehensive cybersecurity strategies that address both technological vulnerabilities and organisational factors influencing cybersecurity effectiveness.

5.10.1 Strengthening Cybersecurity Governance

One of the key implications of the findings of this study is the need for stronger cybersecurity governance structures within mining organisations. Although several organisations have some form of cybersecurity policies in place, the results indicate that these policies are not always

consistently enforced or regularly updated to address emerging cyber threats. Effective cybersecurity governance requires clear organisational leadership, defined security responsibilities, and regular review of security policies and procedures.

Mining organisations should therefore ensure that cybersecurity governance is integrated into overall organisational risk management processes and supported at the executive level. Senior management involvement in cybersecurity decision-making is important because it ensures that cybersecurity initiatives receive adequate resources and organisational support. Establishing dedicated cybersecurity roles or committees may further strengthen governance structures and improve coordination of cybersecurity activities across different organisational units as there are people dedicated to ensure that every aspect of cybersecurity is covered and up to date.

Cybersecurity governance frameworks such as those promoted by NIST emphasise that effective cybersecurity management requires continuous risk assessment, policy development, and monitoring of organisational security practices. Applying such governance principles within mining organisations can help ensure that cybersecurity strategies remain aligned with always changing cyber threat environments.

5.10.2 Enhancing Protection of Operational Technology Systems

The findings also highlight the importance of strengthening cybersecurity protection for operational technology systems used in mining environments. Industrial control systems and automated production technologies play a critical role in modern mining operations, and disruptions to these systems can result in significant operational and financial losses. As mining organisations increasingly integrate operational systems with corporate networks, protecting these environments from cyber threats has become a critical priority in modern mining operations.

Mining organisations should therefore prioritise the implementation of network segmentation strategies that separate OT systems from corporate IT networks. This separation limits the ability of attackers to move laterally across systems and reduces the risk that cyber intrusions targeting

corporate systems will directly affect operational infrastructure. In addition, secure remote access controls should be implemented to manage external connections into the internal networks.

Continuous monitoring of operational environments is also essential for detecting cyber incidents affecting industrial systems. Monitoring tools capable of analysing network traffic, user behaviour, and system activity can help organisations detect suspicious activity at early stages and respond before attacks disrupt operational processes. Firewalls, intrusion detection and prevention systems should always be in place and correctly configured for maximum protection.

5.10.3 Improving Identity and Access Management Practices

Another important implication relates to the need for stronger identity and access management practices within mining organisations. Weak access controls and excessive user privileges were identified as vulnerabilities that could enable both insider misuse and external cyber intrusions. Addressing these weaknesses requires organisations to adopt stricter access management policies and technologies that has central control and visibility of user activity.

The principle of least privilege should be implemented across organisational systems so that employees only have access to the information and systems necessary for their operational roles. Multi-factor authentication mechanisms can further strengthen access control by requiring additional verification steps before granting system access, therefore need to be enforced. These measures hugely reduce the likelihood that compromised credentials will allow attackers to gain unauthorised access to organisational networks since there is an additional level of protection.

Improving identity and access management is always important in mining environments where multiple employees, contractors, and service providers may require access to organisational systems. Effective management of user privileges helps ensure that access rights remain aligned with operational responsibilities and reduces the potential for insider-related security incidents.

5.10.4 Developing a Strong Cybersecurity Culture

Human behaviour plays a central role in many cybersecurity incidents, particularly those involving phishing attacks and credential compromise. The findings of this study indicate that employee awareness and organisational security culture significantly influence the effectiveness of cybersecurity practices within mining organisations. As a result, strengthening cybersecurity culture should be considered a key priority for improving organisational security resilience in all mining operations.

Mining organisations should implement continuous cybersecurity awareness programmes that educate employees about common cyber threats and safe system usage practices. These programmes should include training sessions, awareness campaigns, and simulated phishing exercises designed to help employees be able to recognise and respond appropriately to possible cyber threats. Cybersecurity awareness should also extend beyond IT personnel to include operational staff and management personnel who interact with organisational systems for it to be effective because one weak link can compromise the whole effort.

Developing a strong cybersecurity culture encourages employees to take personal responsibility for protecting organisational information systems. When employees understand the importance of cybersecurity and recognise their role in maintaining security, organisations are better positioned to prevent cyber incidents caused by human error or negligent behaviour.

5.10.5 Strengthening Incident Response and Organisational Resilience

The final implication of the study relates to the importance of incident response preparedness and organisational resilience. Cyber incidents such as ransomware attacks can occur even in organisations with strong preventative controls. For this reason, mining organisations must be prepared to respond effectively to cybersecurity incidents in order to minimise operational disruption and financial losses.

Incident response plans should clearly define the procedures for detecting, reporting, and responding to cyber incidents. These plans should identify the roles and responsibilities of incident response teams and outline communication procedures during cybersecurity emergencies. Regular

testing of incident response plans through simulation exercises can help organisations evaluate their readiness to respond to cyber incidents and identify areas requiring improvement.

Reliable data backup systems and disaster recovery strategies are also important for maintaining organisational resilience in the face of cyber threats. Regularly tested backup systems allow organisations to restore affected systems following ransomware attacks without paying ransom demands or disrupting operations. By strengthening incident response capabilities and recovery mechanisms, mining organisations can improve their ability to maintain operational continuity during cybersecurity incidents.

5.10.6 Strategic Importance of Cybersecurity in the Mining Sector

The implications of this study highlight that cybersecurity has become a strategic issue for the mining sector rather than solely a technical concern managed by IT personnel. As mining organisations continue to adopt digital technologies and automated operational systems, cybersecurity risks will increasingly affect operational stability, financial performance, and organisational reputation.

Mining organisations must therefore adopt a holistic approach to cybersecurity management that integrates governance, technical safeguards, employee awareness, and incident response preparedness. Implementing the cybersecurity framework proposed in this study can support mining organisations in addressing these challenges and strengthening their preparedness against ransomware and insider threats.

In summary, improving cybersecurity management within Zimbabwe's mining sector requires coordinated efforts across organisational governance, technical infrastructure, and human behaviour. By addressing the vulnerabilities identified in this study and implementing structured cybersecurity strategies, mining organisations can significantly reduce their exposure to cyber threats and support the secure digital transformation of mining operations.

5.11 Chapter Summary

This chapter presented the discussion and interpretation of the findings obtained from the empirical data analysed in Chapter 4. The discussion examined the results in relation to the research questions and objectives of the study while linking the findings to existing cybersecurity literature. The analysis provided insight into how ransomware and insider threats affect mining organisations in Zimbabwe and how these threats interact with organisational vulnerabilities and existing cybersecurity practices.

The findings revealed that ransomware attacks are a significant cybersecurity risk in the mining sector, usually originating from phishing attacks and compromised credentials. Insider threats were also identified as an important concern, arising from both intentional misuse of authorised access and unintentional actions such as weak security practices or poor cyber hygiene. These results demonstrate that cybersecurity risks within mining organisations may originate from both external attackers and internal organisational activities.

The study also identified several vulnerabilities that contribute to cybersecurity risks in mining environments. Key weaknesses include use of legacy operational technology systems, weak identity and access management practices, and limited monitoring of organisational networks. In addition, the integration of information technology and operational technology systems increases the complexity of managing cybersecurity risks within mining operations.

Although a number of mining organisations have implemented basic cybersecurity measures such as security policies, firewalls, and employee awareness initiatives, the findings indicate that these measures are not always consistently implemented or adequately enforced. As a result, existing cybersecurity practices provide only a generic level of protection against evolving cyber threats.

Based on the findings, the study identified several important requirements for strengthening cybersecurity resilience in the mining sector. These include stronger identity and access management mechanisms, improved network segmentation between IT and operational systems, continuous monitoring of organisational networks, enhanced employee awareness programmes, and clearly defined incident response strategies. These elements formed the basis of the cybersecurity framework proposed in this study.

Overall, the findings demonstrate that cybersecurity has become a strategic concern for mining organisations as digital technologies become more integrated into mining operations. Strengthening governance structures, improving technical security controls, and enhancing organisational awareness are essential steps for reducing exposure to ransomware and insider threats within Zimbabwe's mining sector.

References

1. Accenture (2024) *Cyber threat intelligence report 2024: Industrial sector focus*. Dublin: Accenture Security.
2. Alsowail, R. and Al-Shehari, T. (2022) 'Techniques and countermeasures for preventing insider threats in organisations', *International Journal of Information Security Research*, 12(3), pp. 142–156.
3. Adu, K. and Darko, E. (2023) 'Cybersecurity readiness in African industrial sectors: Emerging risks and policy responses', *African Journal of Information Systems*, 15(2), pp. 89–105.
4. Baron, R. and Kenny, D. (1986) 'The moderator–mediator variable distinction in social psychological research', *Journal of Personality and Social Psychology*, 51(6), pp. 1173–1182.
5. Broadhurst, R., Grabosky, P. and Alazab, M. (2024) 'Ransomware attacks and cyber extortion: Emerging global patterns', *Computers and Security*, 136, pp. 103–120.
6. Chikosha, F. and Mhlanga, D. (2023) 'Digital transformation and cybersecurity challenges in Southern African industries', *Journal of African Business*, 24(4), pp. 512–529.
7. Clifton, M. (2024) 'Strategies for insider threat mitigation and detection in modern organisations', *Journal of Cybersecurity Practice*, 9(1), pp. 55–71.
8. Cohen, J. (1988) *Statistical power analysis for the behavioral sciences*. 2nd edn. Hillsdale, NJ: Lawrence Erlbaum Associates.
9. Creswell, J. (2014) *Research design: Qualitative, quantitative and mixed methods approaches*. 4th edn. Thousand Oaks, CA: Sage.
10. CSIR (2023) *African cybersecurity landscape report*. Pretoria: Council for Scientific and Industrial Research.
11. Deloitte (2024) *Global future of cybersecurity in industrial sectors*. London: Deloitte Insights.
12. Elmrabit, N., Yang, L. and Kanhere, S. (2024) 'Security challenges in industrial control systems and operational technology environments', *IEEE Access*, 12, pp. 22854–22872.

13. Etikan, I., Musa, S. and Alkassim, R. (2016) ‘Comparison of convenience sampling and purposive sampling’, *American Journal of Theoretical and Applied Statistics*, 5(1), pp. 1–4.
14. Field, A. (2018) *Discovering statistics using IBM SPSS statistics*. 5th edn. London: Sage.
15. Goni, A., Rahman, M. and Chowdhury, N. (2023) ‘Cybersecurity threats, vulnerabilities and prevention strategies’, *Journal of Information Security and Applications*, 72, 103356.
16. Greitzer, F. and Frincke, D. (2023) ‘Combining traditional cybersecurity audit data with psychosocial data: Towards predictive insider threat analytics’, *Insider Threat Journal*, 4(2), pp. 21–36.
17. Hair, J., Black, W., Babin, B. and Anderson, R. (2020) *Multivariate data analysis*. 8th edn. London: Cengage Learning.
18. IBM Security (2024) *Cost of a data breach report 2024*. Armonk, NY: IBM Corporation.
19. Ibiyemi, A. and Olutimehin, O. (2024) ‘Cybersecurity risks in global supply chains’, *Journal of Supply Chain Security*, 6(2), pp. 91–108.
20. Jain, S. and Kotecha, K. (2023) ‘Industrial cybersecurity: Protecting operational technology infrastructures’, *IEEE Transactions on Industrial Informatics*, 19(7), pp. 8501–8510.
21. Kaspersky (2023) *The state of industrial cybersecurity report*. Moscow: Kaspersky Lab.
22. Kaur, P., Singh, R. and Kaur, H. (2023) ‘Advanced cyber threats and cybersecurity innovation’, *Journal of Information Security*, 14(2), pp. 112–128.
23. Khan, M., Salah, K. and Jayaraman, R. (2024) ‘Cybersecurity in industrial Internet of Things environments’, *Future Generation Computer Systems*, 148, pp. 441–456.
24. Lawall, M. and Beenken, M. (2024) ‘A threat-led approach to mitigating ransomware attacks’, *Computers and Security*, 134, 103301.
25. Maphosa, T. (2024) ‘Cybersecurity governance and practices in Zimbabwe’s financial services sector’, *African Journal of Information Systems*, 16(1), pp. 45–60.
26. Masimba, T., & Zuva, T. (2021) Technology adoption models in information systems research: A critical review. *International Journal of Advanced Computer Science and Applications*, 12(4), 306–314.
27. Mhlanga, D. (2023) ‘Industry 4.0 technologies and cybersecurity risks in African economies’, *Technological Forecasting and Social Change*, 189, 122356.

28. Moussaileb, A., Bouguettaya, A. and Chen, S. (2024) ‘A survey on Windows-based ransomware taxonomy and detection’, *ACM Computing Surveys*, forthcoming.
29. Mukucha, T. and Mapuranga, B. (2024) ‘Cybersecurity readiness in Zimbabwean enterprises’, *Zimbabwe Journal of Information Systems*, 7(1), pp. 14–29.
30. Moyo, K. and Madi, T. (2023) ‘Digital transformation and cyber risk in Zimbabwean industries’, *Southern African Journal of Information Systems*, 15(1), pp. 1–13.
31. National Institute of Standards and Technology. (2024). *The NIST cybersecurity framework (CSF) 2.0*. Gaithersburg, MD: National Institute of Standards and Technology.
32. Nunnally, J. (1978) *Psychometric theory*. 2nd edn. New York: McGraw-Hill.
33. Obi, C., Adeyemi, A. and Adepoju, A. (2024) ‘Comprehensive review of modern cybersecurity threats and defence strategies’, *Information Security Journal*, 33(2), pp. 102–118.
34. Oluwafemi, O., Adewale, O. and Salami, A. (2024) ‘Cybersecurity resilience strategies in developing economies’, *Journal of Global Information Technology Management*, 27(1), pp. 67–83.
35. Pallant, J. (2020) *SPSS survival manual*. 7th edn. London: Routledge.
36. Ponemon Institute (2023) *Cost of insider threats global report*. Traverse City, MI: Ponemon Institute.
37. Richardson, R. and North, M. (2023) ‘Ransomware: Evolution, mitigation strategies and defence mechanisms’, *Computers and Security*, 128, 102564.
38. Safitra, R., Ibrahim, M. and Abdullah, N. (2023) ‘Counterattacking cyber threats: A framework for the future of cybersecurity resilience’, *Journal of Cybersecurity Technology*, 7(3), pp. 188–204.
39. Saeed, N., Ahmad, M. and Khan, R. (2023) ‘Digital transformation and cybersecurity challenges for organisational resilience’, *Information Systems Frontiers*, 25(4), pp. 1453–1468.
40. Saunders, M., Lewis, P. and Thornhill, A. (2019) *Research methods for business students*. 8th edn. Harlow: Pearson.
41. Tabachnick, B. and Fidell, L. (2013) *Using multivariate statistics*. 6th edn. Boston: Pearson.

42. Tembo, P. and Phiri, J. (2024) ‘Cybersecurity maturity assessment in Southern African organisations’, *Journal of Information Security in Africa*, 9(2), pp. 55–70.
43. Verizon (2024) *Data breach investigations report*. New York: Verizon Enterprise.

Appendices

**Included separately as attachments*

Appendix 1: Questionnaire form

Appendix 2 : Questionnaire responses