ENHANCING INFORMATION SECURITY AT RZM MUROWA: STRATEGIES, TECHNOLOGIES AND RECOMMENDATIONS.

AFRICA UNIVERSITY–UNITED METHODIST RELATED INSTITUTION

2025

AFRICA UNIVERSITY

(A United Methodist-Related Institution)

ENHANCING INFORMATION SECURITY AT RZM MROWA: STRATEGIES, TECHNOLOGIES AND RECOMMENDATIONS.

BY

RUMBIDZAI CHAKUMARANI

A DISSERTATION PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF BACHELORS IN COMPUTER SCIENCE IN THE FACULTY OF ENGINEERING AND APPLIED SCIENCES.

2025

ABSTRACT

This research delves into the critical area of information security at RZM Murowa, aiming to assess the effectiveness of existing measures and technologies, identifying vulnerabilities, and proposing strategies to enhance its security posture. Qualitative research method, was used in this study to provide a comprehensive understanding of the current state of information security at RZM Murowa. The research began with a thorough review of existing security policies, procedures, and technical documentation. This analysis helped in the identification of gaps or weaknesses in the current security framework. Subsequently, interviews and observations were conducted with key stakeholders, including IT personnel, security experts, and employees, to gain insights into their perceptions of security risks and challenges. The researcher gathered vast amounts of data, in the form of text and audio files, afterwards the researcher presented and analysed the research findings in order to find the areas that needed improvement. Based on the findings of this study, the research proposed strategies to enhance information security at RZM Murowa. These strategies may include; strengthening Access Controls, enhancing Network Security, improving Endpoint Security, raising Employee Awareness, Incident Response Planning and leveraging Emerging Technologies**.** If the company adopts and implement these strategies, RZM Murowa can significantly enhance its information security posture, protect its critical assets, and mitigate the risks associated with information security threats.

Keywords: Information Security, Vulnerabilities, Security Policies, strategies and technologies, information security threats and challenges.

DECLARATION

I declare that this dissertation proposal is my original work except where sources have been cited and acknowledged. The work have never been submitted, nor will it ever be submitted to another university for the award of a degree.

22/03/25

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

RUMBIDZAI CHAKUMARANI DATE

(Student)

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

MRS L.TEMBANI-FUNDISI DATE

(Supervisor)

COPYRIGHT

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my parents, Dr Tracy and Tsuto, for their unwavering support and encouragement throughout my academic journey. Despite the challenges I faced during my time at Africa University, they remained steadfast in their support. I am also deeply grateful to my friends and family for their constant belief in me, their encouragement and understanding have been invaluable in helping me overcome obstacles and achieve my goals.

I would like to extend special thanks to my supervisor at the mine site for their guidance and mentorship. Their expertise and insights have significantly contributed to the successful completion of this research. I am also indebted to the IT Engineer, Douglas Chibiku, and my supervisor, Mrs L. Tembani-Fundisi, for their invaluable assistance in drafting this thesis.

Moreover, I would like to acknowledge the support of RZM Murowa for providing me with the opportunity to conduct this research. I am also grateful to all the participants who generously shared their time and insights, making this research possible. Last but not least, I would like to extend my heartfelt gratitude to Mrs Nyahore, who has been a supportive mother figure since my first day at Africa University. It is through God's grace that I was given the opportunity to attend Africa University.

DEDICATION

To my mom, who encouraged me to soldier on even when the going was not easy….. And to my little self for not giving up!

“*Always Ready To Figure It Out*”

LIST OF ACRONYMS AND ABBREVIATIONS

SETA - Security Education, Training and Awareness

STS - Socio-Technical System

GDPR- General Data Protection Regulation

HIPAA- Health Insurance Portability and Accountability Act

PCI- Peripheral Component Interconnect

DSS- Decision Support System

EDR – Endpoint Detection and Response

IDS- Intrusion Detection Systems

SIEM- Security Information and Event Management

APT- Advanced Persistent Attacks

SCADA- Supervisory Control and Data Acquisition

InfoSec- Information Security

OT- Operational Technology

IoT- Internet of Things

IS & T- Information Systems & Technology

CCTV-Closed-circuit television

USB- Universal Serial Bus

PC- Personal Computer

OS- Operating System

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1: INTRODUCTION

1.1 **INTRODUCTION**

Information security is of very crucial importance for RZM Murowa due to the reliance on technology and the increasing digitalization of operations. Adequate information security is needed to protect the company against cyber-attacks and access to sensitive data (Nieles, 2019). Cyber-attacks such as phishing, malware and ransom ware can have devastating results for both the company and the society as a whole. RZM Murowa specializes in mining and processing diamond and due to the nature and demand of the mineral, information security protocols and systems needs close monitoring and maintenance to safeguard the company from malicious attackers. (Nieles, 2019)

The increase in the number of cyber threats to RZM highlights the need for information security enhancement and proper cyber security hygiene practices to minimise the chances of being compromised. Previous attacks have exposed sensitive data and personnel records which resulted in excessive security costs, and loss of business revenue. The impact of data breaches on individuals can also be devastating, causing financial loss, damage to credit scores, and emotional distress. On another note, there are other information security issues other than security breaches and attacks, power cuts, natural disasters also are a contribution to the disruption of RZM's Information system. Implementing backup system infrastructures is of dire need to the company in case of data loss, it would take time to recover data or might be lost for good causing a business loss.

1.2 BACKGROUND OF THE STUDY

The research was focused on how to enhance the information security at RZM Murowa starting with the security systems, technologies and control measures that are already in use .RZM Murowa is a prominent diamond mining company in Zimbabwe, it handles critical operational, pricing and personnel data which is critical to the everyday running of the company. It is this significance and sensitivity of the data that attracts cyber attackers. The nature of the mineral requires tough physical and digital security to minimize cyber-attacks interrupting the company operations. The increase in the number of cyber threats indicates the need to enhance the security systems because hackers are getting new skills every day to gain access to company resources.

Also natural disasters, power cuts and use of legacy systems are also a disruption to the company information security systems as it poses a great risk of system failure. An example is the failure of air conditioning in the server rooms leading to the failure of the Storage Area Network (SAN). This caused a whole lot of damage, like the cost and time to recover the data affecting business productivity at the mine. The reliance of RZM Murowa on Legacy systems has made it hard to integrate modern security features in the security system since there are not compatible with modern technologies on the market hence making it hard to improve the system.

1.3 Statement of the problem

RZM Murowa as a company deals with the mining of a very lucrative mineral (diamond) which naturally on its own attracts a bunch of malicious attackers. The reliance on interconnected systems in the day to day operations of the company has also rendered the company vulnerable to both internal and external attacks. These attacks ranges from theft, ransom ware, phishing, viruses and Trojan horses trying to get access to company information including pricing data, operational data and personnel data.

As a result, the company needs to adopt new technologies, strategies and control measures to counter for the emerging threats that the company is facing every day and those that haven't surfaced yet but existing. Traditional security systems are proving to be weak day by day as we delve deep into modern technologies were hackers are working very hard to improve their hacking skills on the market every day. This research tried to explore the possible ways to improve the security system at RZM Murowa and gave recommendations.

1.3 Research Objectives

1. To assess the effectiveness of the existing information security strategies and technologies at RZM Murowa.
2. To identify the common types and causes of security breaches.
3. To recommend on strategies, technologies to improve the information security system at RZM Murowa.

1.4 Research Questions

1. What are the current information security technologies and strategies in place at RZM?
2. What are the common types and causes of cyber-attacks or data breaches?

3. What strategies could be recommended to improve the information security system at RZM Murowa?

1.5 Assumptions

1. Assumed that RZM had basic security controls like firewalls and antivirus in place.

2. Assumed that Users are aware of cyber threats within the company and that training programs are being carried out to raise cyber awareness.

3. Assumed that the current data access controls were overly permissive.

4. Assumed that the Murowa community will accept and comply with security changes or enhancements.

1.6 Hypothesis

Implementing a multi-layered security awareness training program for all employees at RZM Murowa will significantly reduce the rate of data breaches within the company.

1.7 Significance of the study

1.7.1 Significance of the study to the researcher

The researcher aimed to gain valuable insights in the field of cyber security in the mining industry. This research allowed the researcher to gain expertise in this specific area, making them a valuable asset in the cyber security field. Furthermore, the researcher aimed to recommend new technologies and strategies to improve or enhance the information security at RZM Murowa.

1.7.2 Significance of the study to the Company

This research helped the company identify some of its vulnerabilities and the possible ways they could adopt to improve their information security posture. This research also helped them to avoid potential harm and reputational damage caused by the realization of threats by the company. It can also help the company to adopt modern information security systems that can incorporate emerging security technologies.

1.8 Delimitations of the study

This research focused on the RZM Murowa information security only and this means that the results of this research are limited to RZM Murowa information security.

The study looked into the enhancement of information security at RZM, strategies, technologies and recommendations.

This study was conducted for 12 months.

1.9 Limitations

1. **Resources**- Budgetary constraints and lack of skilled information security professionals to implement robust security systems can limit the comprehensiveness of the security improvements.
2. **Legacy Systems**- Integrating new security measures with older IT infrastructure might prove challenging.

CHAPTER 2 REVIEW OF RELATED LITERATURE

2.1 Introduction

The mining sector is becoming more susceptible to information security threats as it undergoes digital transformation, merging information technology (IT) with operational technology (OT). As mining operations grow increasingly interconnected and automated, the demand for strong information security practices is more essential than ever. Information security safeguards not just sensitive information but also maintains the integrity of operations. While the merging of IT and OT systems boosts efficiency, it also brings about new risks that need to be handled effectively (Works, 2024).This review of existing literature examined the present state of InfoSec at RZM Murowa, emphasizing key technologies, strategies, and suggestions for improving information security.

Key Information Security Challenges

Outdated Systems- RZM Murowa relies on old information security infrastructure which was designed before the emergence of modern information security technologies. This makes it difficult to merge the systems and these security technologies increasing vulnerability and operational disruptions (Works, 2024).

Increased Attack Surface- The integration of IT and OT has enlarged the range of potential targets for cybercriminals. Due to remote work setups and digital integration, the attack surface has grown considerably, rendering traditional perimeter defences less efficient.

Human Factors: A large number of cyber incidents arise from mistakes made by individuals, including weak password management and insufficient training on cyber security protocols. Tackling these weaknesses is essential for minimizing the likelihood of breaches.

Information Security Threats in Mining Industries

The mining industry is undergoing a significant transformation due to the integration of advanced technologies, which has introduced a range of information security threats. This shift, driven by the integration of advanced technologies, presents a double-edged sword. While it offers significant opportunities for increased efficiency and productivity, it also introduces a complex array of information security threats.

Cybercriminals are increasingly targeting the mining sector due to its reliance on interconnected systems and the value of its data. Ransomware attacks are being carried out to cripple operations by encrypting critical systems, leading to significant financial losses and operational disruptions (Manav, Securing the Connected Mine: Managing Cyber Risks in Mining's Digital Transformation, 2023b). Blair (2024) also talked about ransomware as a strategy designed to extract pay-outs from the attacked entity so they can release the information or decryption key. From both studies, ransomware attacks are there to shutdown critical business systems and cause disruptions which in turn costs the business as the attackers request for ransom to decrypt or release the information.

Furthermore, mining companies possess valuable data, such as geological information and financial records, mineral assays, drilling reports, which can be stolen and misused for financial gain or competitive advantage (Blair, 2024).Another threat is the hacking of industrial control systems, potentially leading to unsafe working conditions, environmental hazards, and significant productivity losses. Leaking of confidential operational information such as production forecasts, equipment health metrics, mine plans can benefit competitors, hampering profitability (Manav, Securing the Connected Mine: Managing Cyber Risks in Mining's Digital Transformation, 2023b).

More so**, t**he global nature of mining supply chains exposes the industry to risks associated with less secure third-party components and services. Also, many mining operations still rely on outdated OT systems that lack modern security features, making them easy targets for information security attacks (Manav, Securing the Connected Mine: Managing Cyber Risks in Mining's Digital Transformation, 2023b).The integration of IoT devices, autonomous vehicles, and remote monitoring technologies expands the attack surface, making it more difficult to secure OT networks (Intelligence, 2022) .In conclusion, the mining industry must prioritize information security to mitigate these risks.

Information Security Exposures

The diamond mining industry faces significant information security exposures due to its unique operational environment and the high value of its assets. These vulnerabilities can be categorized into several areas, including cyber threats, physical security risks, and regulatory compliance challenges.

The reliance on aging operational technology systems like industrial controls and Supervisory Control and Data Acquisition (SCADA).This becomes an exposure in the sense that old infrastructure no longer have the support it had as before, no patch releases making it difficult to secure. They are also not easy to integrate with modern systems posing risks if not configured properly.

According to (Numaan, 2015), the diamond mining sector generates valuable data during exploration and production phases (exploration reports, mineral assays, equipment telemetry data) making it a prime target for espionage. Attackers may seek to steal proprietary exploration data or operational strategies, which can severely impact a company's competitive edge. He further asserts that this is majorly through social engineering attacks or physically stationed agents at the company. Numaan believes that the mining industry has increasingly become susceptible to ransomware attacks, where malicious actors encrypt critical data and demand payment for its release. Such incidents leads to operational shutdowns and significant financial losses and a good example is the Ryuk Ransomware attack on RZM Murowa system.

In a similar incident, RIO Tinto once succumbed to one of the biggest attacks in industry history. In March 2023, personal and family data of employees, payroll information was stolen and published online threatening the safety of their human capital and the corporate reputation at large.

On another note, (Exabeam, What is Information Security (InfoSec)? Goals, types and applications, 2024b) suggests that Advanced Persistent Attacks has become most prevalent in recent years. APTs involve prolonged and targeted attacks where attackers infiltrate systems to gather sensitive information over time. These threats can originate from organized groups, including those backed by nation-states or rival companies. They can also result from a past incident were hackers leave a backdoor to be able to exploit again

Another Exposure is of employees with legitimate access who may inadvertently or intentionally compromise security by leaking sensitive information or engaging in sabotage. This risk is heightened in environments where personnel are not adequately trained in security protocols or where employees are dissatisfied by a company’s treatment of their welfare. (Exabeam, What is Information Security (InfoSec)? Goals, types and applications, 2024b)

More so, diamond mines are prime targets for theft due to the high value of the materials extracted. Unauthorized access can lead to significant financial losses through both external theft and internal pilferage. Physical security breaches may result in vandalism or sabotage of equipment, which can disrupt operations and lead to costly repairs or replacements.

The diamond supply chain is often scrutinized for issues related to human rights abuses and illicit trade. Companies must ensure compliance with international standards, such as the Kimberley Process Certification Scheme (KPCS), which aims to prevent conflict diamonds from entering the market (Chikane, 2011). The company should engage with local community to maintain a social license to operate. Failure to address community concerns regarding environmental impact or economic benefits can lead to unrest and operational disruptions.

Mine sites are also frequently located in remote regions where there is limited physical security with no proper safety equipment and robust information security infrastructure compared to corporate offices. This can hamper access controls, network monitoring and incident response for example intruders.

The diamond mining industry must navigate a complex landscape of information security exposures that encompass both digital and physical threats, alongside regulatory compliance challenges. To mitigate these risks, companies should implement comprehensive security strategies that include robust information security measures, physical security protocols, employee training programs, and active engagement with regulatory bodies and local communities.

Information security awareness

Information security alertness in the diamond mining industry is crucial for ensuring safety, security, and operational efficiency. This concept encompasses the awareness and responsiveness of personnel to potential hazards, both physical and cyber, as well as adherence to industry regulations.

The diamond mining sector faces significant information security threats, including espionage and ransomware attacks. Numaan (2024) emphasizes that companies must cultivate an awareness of information security threats among employees, ensuring they understand the importance of safeguarding sensitive data related to employees, exploration and production. In that same vein, companies should strive to implement robust data protection measures, such as encryption and secure communication channels (example; faxing for confidential documents), is essential for maintaining the integrity of sensitive information during transactions and operations.

The company must also have clear protocols for responding to information security incidents, thus enhancing the organizational resilience. The incident response plan should be well organized, clearly stating the roles and responsibilities of each and every member of the team. Employees should be trained on these procedures to ensure rapid response is there in case of a breach or attack.

Companies should be in compliance with regulations such as the Kimberley Process Certification Scheme (KPCS) which is vital for ensuring that diamonds are sourced ethically and legally. They should also maintain transparency and traceability throughout the supply chain to avoid involvement with conflict diamonds (Chikane, 2011).

Latest Trends in Information Security in the Mining industry

The mining industry is increasingly becoming a target for information security threats, driven by its reliance on digital technologies and the strategic importance of its operations in global supply chains.

Ransomware remains one of the most significant threats to mining operations. Attackers encrypt critical systems, leading to operational downtime and substantial financial losses. For instance, Fortescue Metals Group experienced a ransomware attack that disrupted its operations, demonstrating how such incidents can halt production and impact revenue significantly (Carter, 2016). The high-stakes nature of mining, with continuous production demands, makes it particularly vulnerable to ransomware tactics.

Mining companies possess valuable data, including geological surveys and pricing information, which are attractive targets for attackers. Carter (2016) further supports this on the recent trends in information security attacks which showed an increase in cyber espionage aimed at stealing sensitive operational data for financial gain and competitive advantage. This includes theft of customer information that can be used to undermine sales efforts or manipulate market conditions.

Environmental activists have increasingly turned to information security attacks as a form of protest against mining operations. These hacktivists aim to disrupt operations or expose practices they deem harmful to the environment. Such attacks not only threaten operational integrity but also pose reputational risks for mining companies.

On another note, information security threats are increasingly being introduced through third-party vendors and contractors. Attackers exploit these relationships to gain access to corporate networks, as seen in incidents where vulnerabilities in third-party software led to significant breaches in large mining firms. This trend underscores the need for stringent information security measures across the entire supply chain.

Furthermore, as mining companies adopt more autonomous technologies, there is a growing risk that attackers could hijack these systems. Breaches could lead to dangerous situations involving heavy machinery or automated haul trucks, posing safety risks for workers and potentially causing environmental disasters (Manav, Securing the Connected Mine: Managing Cyber Risks in Mining's Digital Transformation. Future Bridge Mining., 2023).

Additionally, phishing attacks have become more sophisticated, leveraging artificial intelligence tools to create convincing messages that can bypass traditional security measures. These attacks often serve as entry points for more severe cyber incidents, including ransomware deployments and data breaches. The rise of advanced phishing techniques highlights the need for ongoing employee training and awareness programs.

Also, mining operations still rely heavily on outdated legacy systems that lack modern security features, making them prime targets for information security attacks (Manav, 2023). The integration of these systems with newer technologies increases their exposure to threats, as attackers exploit weaknesses in older infrastructure (Tunnicliffe, 2024).

The fluctuating geopolitical landscape has made the mining sector a target for state-sponsored espionage. Countries may seek to gain competitive advantages by targeting mining companies that hold critical resources or technological innovations this trend is exacerbated by tensions related to resource control and economic competition.

The mining industry faces a complex array of information security threats that continue to evolve alongside technological advancements. Ransomware, data theft, supply chain vulnerabilities, and targeted attacks from hacktivists represent significant challenges that require proactive InfoSec security measures.

Factors affecting the implementation of robust information security measures.

The mining industry faces several limitations that hinder the implementation of robust information security measures. These limitations can be categorized into operational, technological, human, and environmental factors. Mining operations often involve multiple sites with varying degrees of connectivity and technology, making it challenging to enforce uniform security protocols across all locations. More so, mining companies operate with decentralized management, leading to inconsistent security practices and difficulties in maintaining oversight of site-specific security measures.

Furthermore, mining operations still rely on outdated industrial control systems (ICS) that were not designed for connectivity, making them vulnerable to cyber threats when integrated into modern networks. The rapid adoption of IoT devices and automation increases the attack surface, creating new vulnerabilities that existing security measures may not adequately address.

The mining sector often struggles with a lack of skilled information security professionals. This shortage limits the ability to implement and maintain effective security measures, as existing staff may lack the necessary expertise. Human error remains a leading cause of security breaches. Insufficient training and awareness programs can lead to vulnerabilities, as employees may not recognize phishing attempts or other social engineering tactics.

Mining sites are frequently located in isolated areas, complicating the deployment of security personnel and technologies. This remoteness can make it difficult to respond quickly to security incidents. Mining operations can be targets for state-sponsored attacks or geopolitical tensions, which can create an unpredictable threat landscape that is hard to defend against effectively.

Implementing comprehensive information security measures can be costly and resource-intensive. Many mining companies may prioritize immediate operational costs over long-term investments in information security infrastructure.

These limitations collectively contribute to the challenges mining industries face in establishing robust information security measures, leaving them vulnerable to various information security threats and operational risks.

2.2 Theoretical Framework

Thomas(2011) introduced Sociotechnical Systems Theory (STS). The STS hypothesis emphasizes the interdependence of social factors (people, procedures, culture) and technical (technology, infrastructure) components within a system. It underscores how crucial it is to match organisational culture and human behaviour with security mechanisms in information security for ideal viability.

Components of the Theoretical framework

Risk management - incorporates activities such as threat identification, risk assessment, control implementation(security awareness training, access controls), monitoring, and improvement (regular penetration tests, continuously adapting to new technologies and emerging threats).One of the main tenets of RZM Murowa is continuous improvement; giving this idea top priority would significantly alter how people follow and comply with security regulations, controls and responsibilities towards cyber hygiene.

Human Factors - Security awareness training, Role-Based Access Control (RBAC) systems, and an Incident Response Plan(IRP) plays a role in minimizing risk of attacks and how to act if attacked respectively..

Technology Stack - Network security, endpoint security, data security, and system hardening remain crucial components of the system. In order to ensure all this, the systems should be compatible with new information security technologies as obsolete or legacy systems might not be able to capacitate it.

Security Culture- Building a culture that prioritizes security through leadership commitment, employee engagement, and continuous improvement.

Strength of this Framework

STS theory provides a holistic view of security, recognizing the importance of social aspects alongside technical controls. Security culture emphasizes the importance of human behaviour and organizational values in achieving strong information security.

2.3 Relevance of the Theoretical Frame to the Study

The theoretical framework establishes the importance of information security in mining and the need for security system enhancement due to the ever evolving threats and data management threats. It also provides a foundation for the researcher's approach to enhancing security at RZM Murowa by highlighting the importance of minimizing information security risks through strategic planning, awareness training, proper policy dissemination and employing integrated information security infrastructure. Striving to instil a culture of security in every employee at RZM Murowa. More so, it also underscores the need for a risk-based approach to security and a layered security strategy approach with various controls to improve security.

All in all, as mentioned by Thomas, (2003), information security is a combination of efforts towards achieving security and because of that it is everyone's responsibility to ensure that the organization's information security infrastructure and data are not compromised.

Definition of Key Terms

Information security- is the protection of important information against unauthorized access, disclosure, use, alteration or disruption.

Vulnerability- is a weakness that can be exploited to gain unauthorized access to information systems.

Threat- it is an activity, deliberate or unintentional, with the potential to disrupt or harm an information system.

Security measures- This are precautions and steps taken to safeguard information resources from unauthorized disclosure, access and modification.

Summary

This chapter provided a clear walkthrough into the importance of information security and the need to improve the security systems to minimize the risk of cyber threats. It also pointed out some possible solutions to mitigate risks associated with lack of proper information security investment

CHAPTER 3 METHODOLOGY

1.6 Introduction

The diamond mining industry, like many others, faces a growing challenge in securing its information systems. The adoption of innovative technologies like cloud computing and block-chaining can streamline operations and offer remote management capabilities but also introduces new vulnerabilities. While existing research emphasizes the critical role of information security in mining (Mishchuk, 2021; Kirenberg, 2020), there's a lack of studies specifically addressing the information security needs of diamond mining companies, like RZM Murowa.

Additionally, the study aimed to evaluate the effectiveness of existing security measures and recommend improvements based on best practices. The primary objective of this study was to develop a comprehensive strategy to strengthen information security at RZM Murowa. This involved identifying the most critical security risks specific to the mine's operations and technological environment.

1.7 The Research Design

In order to achieve these objectives, a qualitative approach was employed. Data was gathered through structured interviews with key personnel from IS & T departments at RZM Murowa and participatory observations. These interviews delved into current information security practices, employee awareness levels, and perceived security risks specific to the diamond mining industry. On the other hand, observations were also used to gain a good understanding of the information security posture, measures, infrastructure, awareness and the technological gaps to be addressed.

The chosen methodology was well-suited for this study due to its comprehensive nature. Interviews provided valuable insights into employees' perspectives and experiences regarding information security within the diamond mining context. The observations allowed for first hand data to gauge overall security awareness across the organization. Combining these methods enabled a thorough evaluation of the current state of information security and inform the development of a holistic improvement strategy. The subsequent sections of this chapter elaborates on the chosen data collection methods in detail

1.8 Population and Sampling

Bhandari, (2023) defines population as the entire group of elements under study where the research findings will be applied to. A sample are the specific participants or elements from the population that the researcher will collect data from. This is the third part of the research methodology, and the researcher made use of systematic and purposive sampling which is a qualitative method of sampling. This helped the researcher get a deeper understanding of the system from those directly involved in managing and monitoring them.

Qualitative research often employs non-probability sampling methods, which do not rely on random selection. The researcher used purposive and stratified sampling techniques. The researcher grouped the population by strata (departments) and from each department, the researcher purposively chose the appropriate individuals for the sample.

Stratified sampling

This technique involves dividing the population into subgroups (strata) and then sampling from each subgroup to ensure representation across key characteristics such as gender, age, roles. This promoted the diversity of perspectives collected in this qualitative study.

Purposive Sampling

This technique involves the selection of participants who can provide rich, detailed information relevant to the research question. Researchers define specific criteria that participants must meet, ensuring that they have relevant experiences or insights about the phenomenon being studied. For instance, in this study the researcher purposely chose employees who had access to IT systems and services who understands the need for information security.

This study focused on the information system and technology (IS &T) department personnel (system administrators and engineers) of RZM Murowa and a few users from the employees side (system users).

3.4 Data Collection Instruments

3.4.1 Interviews

The APA Dictionary of Psychology (7th ed.) defines an interview as "a structured conversation aimed at eliciting information from an individual" (APA, 2019). It is a qualitative data collection technique used to carry out an in-depth study on a smaller number of respondents to get a deeper understanding of a particular situation or idea. Interviews are of three types, structured, semi-structured and informal. In this research, the researcher made use of structured interviews with pre-set questions in order to get all the information without leaving detail. It allowed the researcher to read non-verbal cues that helped the researcher to assess the responses. The interviews were timed and the minimum time limit was 15 minutes and maximum was 45 minutes.

3.4.2 Observation

It is a participatory study where the researcher has to immerse themselves in the natural setting where their participants are (Dudovskiy, 2021). It is a qualitative method of data collection tool, the researcher observes for example actions, trends, recordings surrounding the object under study. The researcher used systematic observation to study the different threats that threaten the company’s information system and the frequency of their occurrence. Additionally, it helped the researcher to have first-hand information and evaluation, however, it can be researcher biased too.

3.6 Data Collection Procedure

Data collection is the planned process of gathering information from participants or objects to answer research questions" (Muenchen, 2011, p. 17). The researcher conducted in-depth interviews with the participants and collected data. The interviews were in two forms, the physical and telephone interviews. Physical interviews were conducted with the interviewee’s that were in the interviewer’s reach and those outside the researcher's reach were contacted via the telephone. Also the researcher used the results obtained from the observed information system security audit trails, log reports and firewall alerts and reports. The researcher also observed the behaviour of the RZM Murowa employees’ towards security, that is, adherence to security controls and information security policies. Data collection was done using English as the common language to both the participants and researcher.

3.7 Analysis and Organization of Data

Data analysis is the systematic process of inspecting, cleaning, transforming, and modelling data to extract meaningful information, identify patterns, and inform conclusions ([Paulson, 1997]).

The researcher made use of a notepad and call recordings to analyse and document the data gathered during the interviews. Then the researcher transcribed the data, making a clear, readable and meaningful transcript taking note of all the relevant data. The data was coded for easier analysis and for the purpose of drawing conclusions. Thematic analysis was used to gain the understanding of the responses of people from a mining sector security perspective. Thematic analysis involves the identification, analysis and interpretation of recurring themes and data patterns aimed at uncovering underlying meanings, ideas and concepts within a data set (Nicolas & Nicolas, 2023). Afterwards the results were organized in the form of tables, bar graphs and charts to have a detailed explanation of the results of the study.

3.8 Ethical Consideration

1. Participants willingly provided the responses they felt comfortable with and they were free to withdraw anytime they felt they no longer wanted to participate.

2. The researcher did not ask for any personal information that was not related to this study or in any way provoked the interviewee.

3. The researcher respected the principle of confidentiality (privacy) and generalized the findings.

4. The information gathered from this research is for the purpose of learning and no other interest was fulfilled using this dissertation.

5. The researcher held the information gathered with integrity, not altering any of the responses given in any way in respect to the company policies and IT codes of conduct.

3.9 Summary

In this chapter, the researcher explored the methods and techniques of how this study was conducted. This study was a case study research design with the quest to obtain a deeper understanding of the existing information security systems at RZM Murowa and the possible strategies and technologies it would adopt to enhance its information security posture. The researcher also highlighted the possible questions that would be asked in order to understand, assess and give recommendation to the overall RZM Murowa Information security.

Chapter 4: DATA PRESENTATION, ANALYSIS AND INTERPRETATION

4.0 Introduction

This chapter served as the foundation for understanding the strategies, technologies, and recommendations developed from the data findings that have been gathered from the research through the analysis of the interview data using the Sociotechnical System Theory (STS)

The researcher used the research objectives mentioned earlier in the proposal to gather comprehensive insights on the security posture of the organisation (infrastructure, technologies, vulnerabilities and measures in place to protect information security). In depth interviews and structured observations (firewall reports and threat findings, anti-virus alerts, log files from the registry systems, employee behaviour towards policy compliance) were employed to collect data from employees of various departments. The collected data was then processed, analysed, and interpreted using thematic analysis, tables, charts and graphs. The results obtained from this analysis provided valuable information on the key research questions and objectives of this study.

This chapter is organized into sections, each focusing on a specific aspect of the data collection, presentation, analysis, and interpretation process. By examining the findings in detail, this chapter contributes to a deeper understanding of the challenges and opportunities associated with enhancing information security.

4.1 Findings

4.1.1. Sample Profile

Targeted Sample	Interviewed
50	35

Table 1. Response Rate 1

4.1.2 Response Rate

The researcher had targeted 50 people (sample) to interview from the RZM Murowa Organization at the mine site in Zvishavane and the Harare offices. Purposive sampling was used by the researcher to choose eligible interviewees who would understand the information security systems better according to how familiar they're to the systems in use. Interviews were scheduled and done successfully by 35 of the research participants from different departments in Harare and Zvishavane. However, due to the nature of the workplace (most of the work is practical and is done in different shifts), time limitations, resignation of some of the participants, change of work shifts and reluctance to participate by some of the interviewees from the targeted sample, the 50 target could not be reached. The response rate of 76% was attained from the total sample. This gave the researcher a green light to proceed since the response rate was tolerable.

4.1.3 Sample Adequacy, Reliability and Validity

Although the researcher could not reach the targeted sample for interviewing, the participation rate of 76% among the target population sample is still considerable and should provide a diverse range of perspectives from different departments of the company. All the interview templates used where the same for all participants and the time frame for each scheduled interview was also observed to ensure consistency and reliability. Also, the participation of people from different departments at the mine site and Harare office, IS &T, Procurement, Human Resources, Technical Services, HSEQ, Mining and Engineering improves the validity of this study by capturing the different opinions in regard to the subject under study.

4.2 Demographic Characteristics of Research Participants

4.2.1 Gender Distribution

There was a total of 8 women who participated in the interviews which makes 21% of the total percentage of responses. The remaining 30 were males who made up the 55% of the gender distribution. The lower number of respondents from the women indicates the nature of the mining environment which is predominantly occupied by male employees than females.

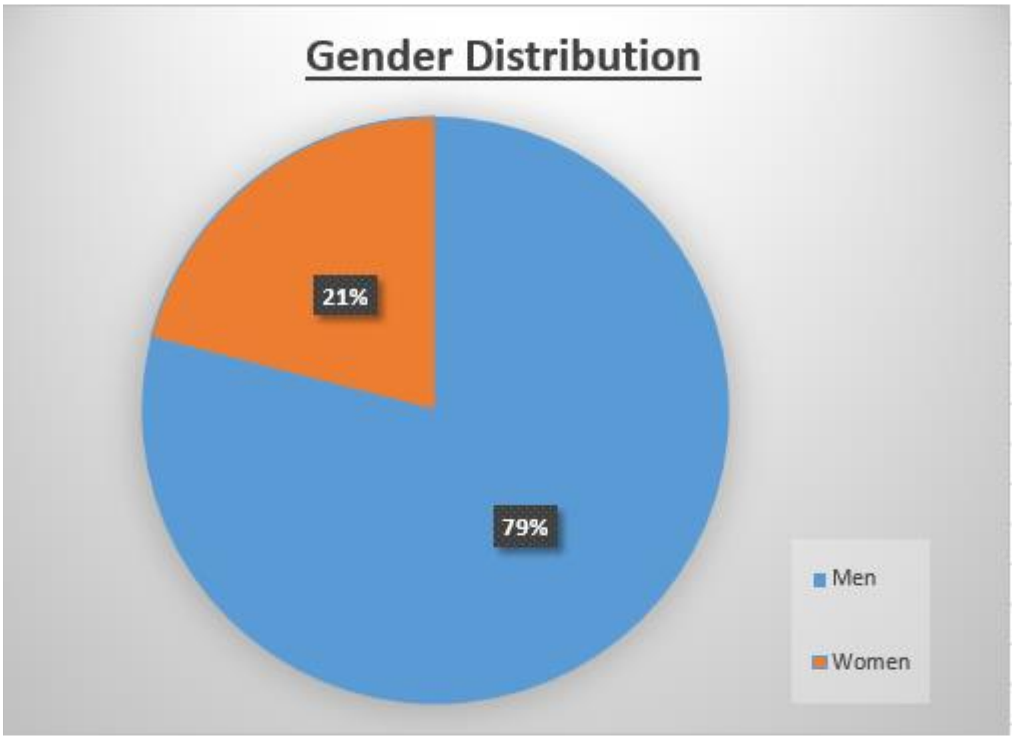


Figure 1. Gender Distribution 1

The main and highest level of qualifications of the respondents were graduate degrees, followed by diplomas, certifications and lastly master's degree holders.

Gender	Qualification	Total
Male	certificate	4
	diploma	5
	Degree	20
	Masters	1
Women	certificate	1
	diploma	1
	Degree	5
	Master Degree	1

Table 2. Qualifications

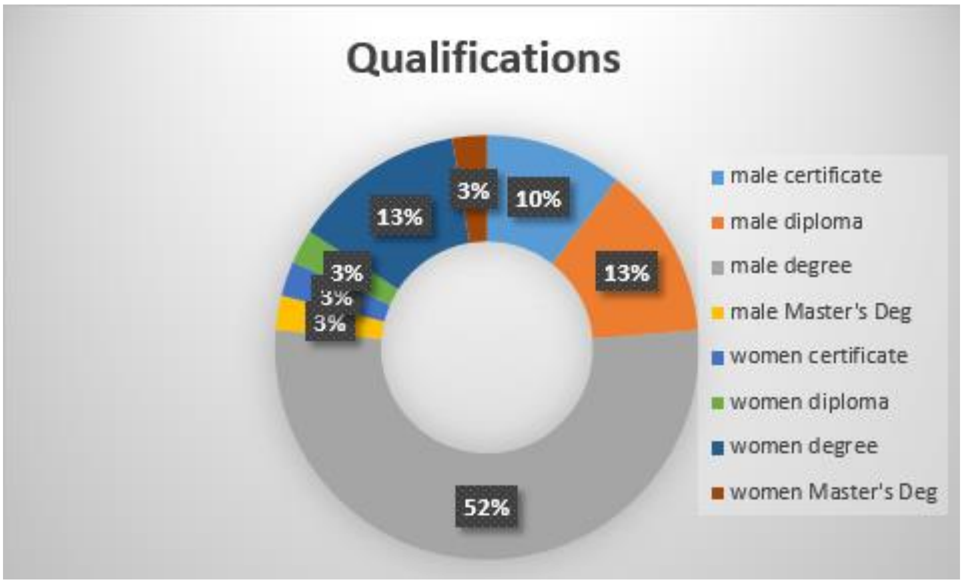


Figure 2. Educational Qualifications 1

4.2.3 Respondents Distribution by Department

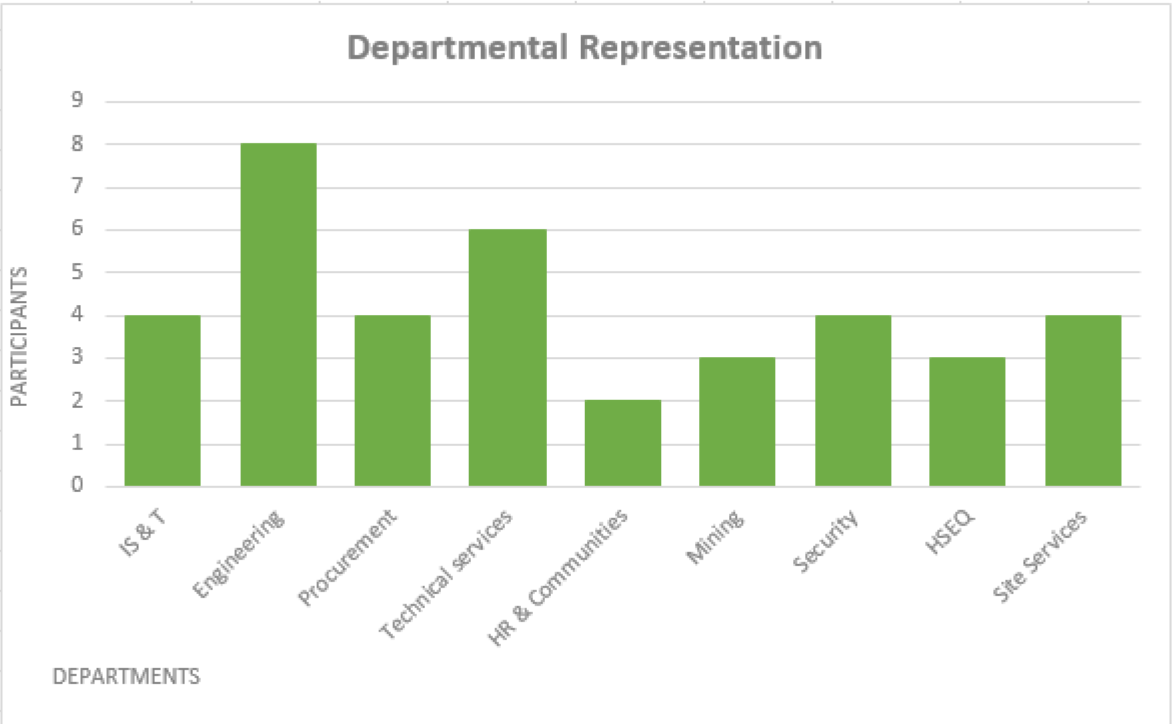


Figure 3. Departmental Representation 1

4.2.4 General understanding of Information Security

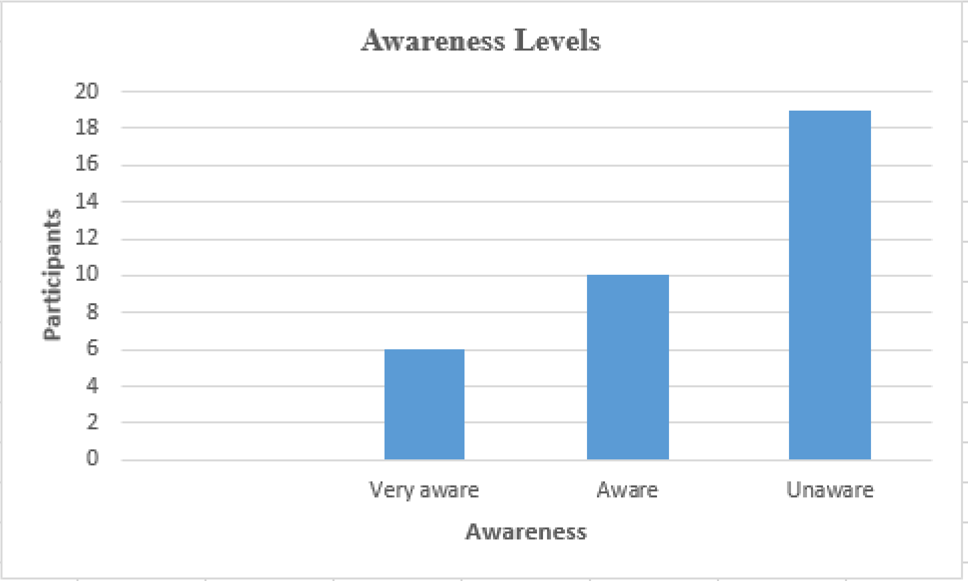


Figure.4 Awareness Levels 1

This section is meant to understand the different levels of information security knowledge among employees in different departmental roles at RZM Murowa. A few people showed a deep understanding of what information security is, indicating a high level of awareness and understanding of information security. On another note, some of the respondents expressed being familiar with information security although their knowledge was not very detailed while the rest of the participants showed that they are not very acquainted to information security and this indicated that there is a wide gap in training and awareness programs on information security procedures and policies and also the general knowledge of protecting information security systems.

4.2.5 Responses to define Information Security

Key responses to define information security from the participants	
1	These are measures and practices to safeguard, confidentiality, integrity and availability of information
2	It involves the protection of information from unauthorized access, use, disclosure or destruction
3	Protecting both company and personal information
4	The safety of online information as well as any data that on generates, have should be secure.
5	It entails that information and data is kept within the confines of those in need or authorised to use it.

Table 3. Key Information Security Definition 1

4.2.6 Primary Information Security challenges faced by RZM Murowa

Observational Data

The researcher observed that the company uses unlicensed software and has poor patch management

Lack of information security training and awareness sessions

Less support from the top management on issues to do with information security awareness, infrastructure and policies.

Use of outdated infrastructure such as desktops, laptops, servers, autoloader and cooling systems

Use of own devices is also one of the concern the researcher observed, it brings vulnerability to the company's information security as the confidentiality and integrity of the data is not guaranteed.

Interview Data

The respondents reported to have experienced a number of phishing attempts in their mailboxes.

The participants also said there is a gap in information security awareness and training because from a previous phishing simulation, some employees clicked the links and got trapped indicating that there is need for robust information security training and awareness.

The use of own gadgets is also a challenge as it exposes the company to many vulnerabilities (insider threats) such as blackmailing.

Participants also highlighted the use of old information security infrastructure as a hindrance to efficient production and a source of security vulnerability as outdated systems lack updates and patches.

Integrated Analysis

Challenges faced by RZM Murowa	Description
Old IT Infrastructure	Infrastructure has reached end of life support, training.
Insufficient security measures	Poor patch management, use of unlicensed software
Use of own gadgets at work	Insider threats, introduction of malware files
Data breaches	Information ending up in the hands of an unauthorized person because of non-compliance to IT policy and procedures
Malware threats	Insiders and externals trying to penetrate or compromise the company's information systems
Training & Awareness	Users should be taught on how to follow IT security policies and procedures and how to use the different applications and all associated tools.

Table 4. Information Security Challenges

As illustrated in Table 4… above, RZM Murowa is grappling with a number of significant information security challenges. Foremost among these is the reliance on outdated infrastructure that is no longer supported, lacking essential security patches and updates. This antiquated technology renders the company susceptible to both internal and external threats, jeopardizing business continuity and potentially disrupting production. Additionally, the company is confronted with the pervasive use of personal devices, such as USB drives, computers, and smartphones, for work-related tasks. Despite a prohibition against such practices, enforcement is hindered by a dearth of IT resources, leaving the information security system vulnerable to exploitation.

4.2.7 Information security training and awareness.

Observational Data

Observed minimal use of strong passwords and password managers among employees

The researcher also noticed a lack of regular security awareness training sessions

Observed the use of unlicensed software and operating systems.

Interview Data

Interviews highlighted the lack of information security education, awareness and training of employees and Information security ambassadors in various departments in the workplace.

Some employees admitted that they click some links because they are not aware of the consequences associated with it … Basically they don’t know what phishing is and how it takes place.

The few top management officials the researcher interviewed showed that they had little to no knowledge of how information security works. This is very worrisome because they are also the ones who deal with bulky, sensitive and confidential information and data of the company. This indicates the need for a comprehensive approach to training and awareness events.

Integrated Analysis

The combination of observational and interview data suggests a significant gap in information security awareness and training at RZM Murowa. The lack of strong password practices and the susceptibility to social engineering attacks highlight the need for regular and effective security awareness training. According to the 35 interviewed individuals, training and awareness on information security programs remains a gap. Employees have insufficient awareness of security risks and best practices. In order to boost information security among employees, the organization should implement comprehensive training programs that cover security best practices, threat awareness, and data protection policies. Additionally, implementing robust access controls, such as multi-factor authentication and role-based access, can help prevent unauthorized access to sensitive information. Finally, the top management employees should take part and support information security by prioritizing it in terms of resource provision and policy making and also encouraging employees to report suspicious activities and providing clear incident response procedures that can facilitate timely detection and mitigation of security breaches.

4.2.8 Information Security Incidents at RZM Murowa

Observational Data

The researcher observed that employees were using personal devices to access company emails and sensitive documents. Also gadgets like external hard drives, USB drives were being used to share information among individuals.

Lack of power redundancy as some of the infrastructure failed because of power cuts.

Financial constraints to maintain and upgrade the server room equipment and cooling systems (air cons).

Interview Data

A senior employee stated, "We've had a drastic information security incident four years back that rendered the company’s critical information inaccessible, interrupting business operations”. This incident was recognized as the RYUK ransomware group attack.

Some participants also highlighted a security breach were employee data was leaked and started circulating online.

Type of breach	Causes

Ransomware	Supply chain vulnerabilities, insider threats, hacking attacks
Data leaks & theft	Employees sharing log in credentials, weak passwords, physical theft of devices
Data exfiltration	Insider threats, malware infections, human error
Unauthorized access	Social engineering techniques, malware infections, misconfiguration of systems.

Figure 5. Security Incidents

In February 2020, RZM Murowa experienced a significant information security breach when the Ryuk ransom ware group compromised its systems, resulting in the encryption of critical data and a disruption of business operations. The attackers demanded a ransom payment for the decryption key, highlighting the vulnerability of the organization's infrastructure to such attacks. Additionally, recurring failures of the Storage Area Network (SAN) due to power outages further compounded the company's operational challenges. Respondents indicated that the recovery process following the Ryuk attack took approximately half a week, while SAN failures typically required one to two days to resolve. The incident also underscored the risk of data breaches, with the potential for sensitive company and employee information to be leaked, leading to blackmail and other adverse consequences. Furthermore, the researcher realized an increase in phishing emails being send to employee email accounts and the different malware and Trojan horses that are detected by the fire wall and antivirus before causing any harm to the systems. These events clearly necessitate a substantial enhancement of the company's information security infrastructure to mitigate the likelihood of future incidents happening and protect its valuable assets.

Integrated Analysis

These findings suggest a lack of awareness and adherence to information security best practices, potentially leading to data breaches and unauthorized access. It is this human capital that needs to be responsible to curb social engineering attacks, minimize phishing attacks and adhere to best information security practices

4.2.9 Importance of Information to RZM Murowa

Observational Data

The researcher observed that the company has poor policy dissemination, enforcement practices, as such, it is difficult for the users to comply with some of these policies.

For instance it was observed that system users were reluctant to create unique and stronger passwords, after they are given the initial password by the system administrators, they continue using it.

There are also no penalties for non-compliance to policy.

Interview Data

Respondents highlighted that information security is crucial in safeguarding the company's interests, operations, exploration data and employee data.

One of the managers emphasized, "Information security is paramount for our operations. A breach could lead to significant financial losses and reputational damage."

Integrated Analysis

While the importance of information security is recognized, there is a need for more concrete policies and procedures to ensure its effective implementation. Information security is crucial for RZM Murowa due to its role in protecting intellectual property, ensuring data privacy and compliance, maintaining operational continuity, mitigating risks, complying with regulations, building investor confidence, and safeguarding supply chain security. By investing in robust security measures, the company can safeguard its valuable assets, minimizing disruptions, and maintaining a strong reputation in the mining industry. All in all, the company's information security is important in protecting the privacy of personnel, company information, ensuring high availability of critical systems and processes in support of the organizations mission.

4.2.1.1 Challenges associated with compliance to IT security procedures and policies

Challenge	Description
Unintentional violation	Mostly due to lack of knowledge and training.
Substantial delays in logging in to the internet	Frequent occurrences of slow internet authentication processes, resulting in extended network connection periods and hindering efficient workflow
Technological integration	It is hard to integrate technologies due to the existing policies and procedures.

Table 6. Compliance challenges

4.2.1.2 Information Security Technologies strategies and Measures

Observational Data

The company has good physical security infrastructure comprising of guards, biometrics (fingerprints and face recognition), perimeter fence, CCTV Surveillance and turnstiles to control access to sensitive areas of the mine site such as the sort house, recovery plant, server rooms and the mine site as a whole.

Technology wise, the researcher observed that Sophos antivirus software was being used on many company machines, along with a Fortinet firewall which has certain features that detects and prevents unauthorized and malicious activities.

Also policies and administrative controls were being used to control access to digital information in the file servers and company machines.

The use of firewall authentication when logging in to the internet is helping the Information security officers to track user activities and monitor the network infrastructure of the company.

Interview Data

Participants highlighted the issue of budgetary constraint as a hindrance to implement more robust information security infrastructure that is more recent and effective.

The researcher also realized that as long as the top management is not involved in the information security discussions, they will not understand the criticality of upgrading the current information security infrastructure and enforcing and prioritizing information security will remain a gap that needs to be addressed.

One respondent said “The Company really needs to make sure that we pay for information security services on time because it is these unlicensed and pirated systems that expose our systems to threats”

Integrated Analysis

This suggests a lack of investment in up-to-date security technologies, which can leave the organization vulnerable to emerging information threats. This necessitates the need for a dedicated information security budget to carter for the system upgrades, penetration tests, licensing fees. However, as it stands the measures and technologies in place have been working well.

4.2.1.3 Effectiveness of current information security measures

Technologies & Measures

Technology/ Measure	Description
Fire wall	RZM Murowa uses a Fortinet firewall to filters and monitors inbound and out-bound network traffic
Antivirus	The company uses a Sophos anti-virus which helps in detecting malicious files and events on the network.
Passwords	Passwords are used to verify (authentication) the identity of a user on the network and give access to resources.
Access Control	This is used to control access to company resources, the company uses role-based access, meaning that everyone has a different level of access to resources in order to safeguard information security.
Back up	The company's IS & T Department run differential and full-back ups, daily and weekly respectively.
Biometrics • **Face recognition** • **Finger prints**	• This technology is used to control access to sensitive areas at the mine and also for identity verification when entering the Minesite and Harare offices. • Are mainly used were entry is restricted to specific personnel of the company and also when accessing sensitive areas like the server room, sort house and plants. They are used in

	conjunction with other technologies such as badges and face recognition.
Badges	They are used in conjunction with finger prints and face recognition for authentication.
Turnstiles	They are used in conjunction with face recognition to have controlled access to the Minesite.
Guards	They are physically stationed in areas that almost every personnel have access too, to monitor their movement and behaviour and also to conduct search.
Fences	Used to mark the boundary between the company and the community and to make it easier to protect the territory.

Table.7

Strategies

Strategy	Description
Policies and procedures	There are various policies that are followed at RZM Murowa in regards to information security. An example of the policies is the prohibition on using the company IT resources for doing business, politics or charity works.
Pre-employment background checks	The company requires un signed finger print forms to track your criminal record and also do checks on your social media posts.
Incident report planning	The company maintains a clear reporting procedure and specifies the roles and responsibilities of each personnel.

Table. 8

Observational Data

During a maintenance activity, the researcher realized that some of the servers they were using were outdated posing as a vulnerability to the company.

Monitoring the mail security system, there are many attempted phishing email attempts, indicating the effectiveness of this mail security feature in detecting malicious mails. However, some phishing emails get through this layer prompting the alertness of the user to differentiate between an authentic email and a malicious one.

Logs from the firewall shows numerous attempts of unauthorized access, however, the firewall is proving to be effective with excellent configurations and administrative controls.

Interview Data

An IT technician reported, "Our current firewall and antivirus software are working well, the only threat we have now is our physical infrastructure at most, using outdated PCs that is not compatible with latest OS and security technologies"

The researcher got similar responses from all the participant pointing towards the outdated infrastructure.

Additionally, the interview highlighted the need for network segmentation to prevent adverse attacks to the whole system.

Integrated Analysis

The current measures are effective since there is no recent incident related to information security. However, there is room to improve the current information security to suit the environment the company is operating in. The researcher observed that the company has not done any training in regard to information security awareness recently (for the whole year the researcher was at the company). This indicates a very big gap in the company's information security since most breaches are either directly or indirectly related to human errors. Using passwords, firewalls, access controls and antiviruses has proven to be effective, however, implementing measures such as multi factor authentication, AI technology and block chain security can significantly improve the company’s information security posture. Integrating the current information security with latest security technologies needs new infrastructure that is compatible with the security tools available in the market. The first goal therefore is to upgrade the information security infrastructure and provide resources for SETA programs. Overall, the current technological infrastructure and security measures appear to be inadequate to address evolving information security threats.

4.2.1.4 Incident Reporting Procedures

Observational Data

At RZM Murowa if one finds out that they have done something that has a potential to render the information security of the company vulnerable, they should report directly to the responsible personnel.

The use of near hit cards also plays a part in incident reporting if the procedure is being well followed. Depending with the impact the incident has on information security one can choose either too report directly or anonymously due to the repercussions associated with it.

The researcher, had been attached to the company for a whole year and never come across an Incident Response Plan (IRP) or just a reporting procedure, there was never a training on this procedure and also a deep research into the previous events, there was no recent training on incident report or response**.**

This highlights how the information security incident response plans are outdated and not up to date.

Interview Data

Employees expressed uncertainty about the proper procedures for reporting security incidents. Some participants showed that they fear the repercussions that comes with reporting an information security incident especially if they are involved in fear of losing their jobs.

Integrated Analysis

A lack of clear and effective incident reporting procedures can hinder timely response and investigation of security incidents. Leaking company information to the external world is a violation of policy on its own because that information can be used against the company for malicious intentions. The company could have a sort of penalties in order to minimize such incidents. Although there is no a clear path to report a security incident, from a perspective of an information security personnel, it is wiser to report directly and immediately to IT and security so as to curb further damage or staying alert.

4.2.1.5 Information Security Concerns

According to the participants' responses, the company is more concerned about the outdated information security infrastructure being used. The use of old infrastructure has increased threat and vulnerability landscape exposing the company's information assets to attackers. The old systems are no longer being updated nor patched since new patch and update releases are not compatible with the system which means that there is no support in case something happens. Lack of resources for upgrading the system, training and awareness of staff and buying software licenses is also a concern for the company. Tabulated below are some of the concerns that the researcher found.

Problem	Concern

Cracked/pirated systems	They have neither updates nor patches making them easier to compromise.
Public Folders	Risk of company information and personal information being leaked violating the confidentiality principle
Passwords	Use of weak passwords by some staff members and the reluctance to change the default password to a more stronger password to make it hard to crack
Legacy Systems	They are no longer supported, with no updates and patch releases
Human Errors	Need for regular training and awareness sessions on information security and proper policy dissemination and compliance.
Use of own devices at work	May lead to both external and internal attacks due to the ease of access, transmission of information between company and personal gadgets.

Table.9 Information Security Concerns

4.2.1.6 Strategies, Technologies and Recommendations that can be incorporated to enhance the already existing information security.

Based on the thematic analysis, the following strategies, technologies, and recommendations can be proposed:

1. **Awareness and Training:**

   Conduct regular security awareness training for all employees.

   Develop clear and concise information security policies and procedures.

   Implement a strong password policy and enforce multi-factor authentication.

2. **Technology Implementation:**

   Upgrade firewall and antivirus software to the latest versions.

   Implement intrusion detection and prevention systems (IDPS).

   Deploy network segmentation to isolate critical systems.

   Utilize encryption technologies to protect sensitive data.

   General system upgrade like using the latest windows version

3. **Incident Response:**

   Develop a comprehensive incident response plan.

   Establish clear incident reporting procedures.

   Conduct regular security audits and vulnerability assessments.

Technologies	Strategies	Description
Multi-factor authentication		It is a security protocol that requires users to provide more than one form of identification to access an account an example is the CISCO DUO application.

Security Information and Events Management software		A software used to collect, analyse and correlating security events from various sources and help identify threats and their patterns an example is Splunk.
Block chain Technology		It provides a secure and transparent way to protect intellectual property .Examples of such software are IPChain and VeriBlock.
	Maintaining integrity of software supply chain	Involves risk assessments, vendor due diligence, component security and technologies used in the supply chain.
	Security Awareness and Training	Invest in Security Education, training programs to make information security a responsibility for everyone.
	Investing in the latest information security technologies and infrastructure	Upgrading the information security infrastructure and buying latest security software. For example cloud computing.
	Honey Pots	Intentionally leaving vulnerable computers to attract attackers then use that information to harden your security systems
	Penetration tests	Regularly testing, analysing and monitoring your systems for vulnerabilities.

Table.10 Recommendations

The figure above highlights some of the possible strategies and technologies that can be adopted by the company in order to enhance its information security.

4.2.1.7 Conclusion

In summary, the findings of this research highlighted the strategies, technologies and recommendations that can be used to enhance the already existing information security at RZM Murowa. In-depth interviews and participant observation were used to analyse and understand the organizations information security posture. Through the analysis of the different responses from the participants and what the researcher observed, different insights emerged that could be incorporated to improve information security. Technologies such as block chain security, multifactor authentication and cryptography were suggested as points of improvements. In this same vein, participants also mentioned different strategies that could be adopted to enhance the information security at RZM Murowa, with training and awareness as the leading way, use of honey pots and penetration test to strengthen the information security posture of the company. However, the challenge to carry out all the above mentioned strategies and technologies lies in the lack of funds to support and upgrade the company infrastructure so that it becomes compatible with latest security technologies. Another challenge is not prioritizing information security as the business runs its day to day operations only realizing the importance after an unfortunate event has happened such as the one in February 2020 when the company information assets were rendered in accessible by RYUK Ransom group. Security Education, training and awareness programs remains a gap.

Chapter 5: SUMMARY, CONCLUSION, AND RECOMMENDATIONS

5.1 Introduction

This chapter explored the implications of the findings on strategies, technologies and recommendations, with a focus on the key findings, conclusions and recommendations derived from the research on RZM Murowa.

5.2 Discussion

Based on the findings, of the research, this section addressed the research problems, objectives, significance, assumptions, delimitations, limitations and key findings on enhancing information security at RZM Murowa as stated in chapter 1. The introduction highlighted the need for enhancing information security, strategies, technologies and recommendations. Study objectives and questions were clearly stated giving the researcher a guideline on how the research had to be conducted and which specific areas to probe. Limitations and delimitation were highlighted giving a clear scope of the study. In addition, key terms were defined to provide clarity throughout the study.

Moreover, chapter 2 provided a review of related literature to establish a foundational understanding of information security and how it was addressed during that time. Socio-Technical Systems Theory, which is an organizational theory that conceptualises a given system in view of its constituent social and technical subsystems, with the goal of achieving system support through joint optimization. It highlights the relation between the social behaviours and culture of the people using the systems and the technology being used. In this context, a culture of security awareness and a sense of responsibility should be instilled in all the employees to have a better information security posture.

In addition, Chapter 3 explored the research methodology used by the researcher to find the different strategies and technologies that could be used to improve information security at RZM

Murowa. The chosen methodology, qualitative research method, research design, data collection procedures and ethical considerations were detailed. This chapter served as the blueprint for the subsequent chapters, providing a robust framework for data synthesis, analysis and interpretation.

Chapter 4 presented the research findings using thematic analysis and also it investigated the effectiveness of user education programs in reducing the risk of phishing attacks. This chapter evaluated different training methodologies, information security infrastructure, password management, strategies and technologies to enhance the information security defences and the impact of user behaviour in enhancing security. Key aspects explored include:

- User Awareness and Behaviour Change- The improvement in user awareness and the reduction in susceptibility to phishing attempts through training and awareness sessions.
- Information security infrastructure- Prohibition of bringing own devices for work related tasks and upgrading the old infrastructure.
- Technologies and strategies- Technologies such as block-chain security and Cloud security adoption to improve security posture. Proper policy dissemination and enforcement to ensure compliance to security.

5.3 Recommendations

A robust information security program is essential for the organization to protect their sensitive data and infrastructure from various threats

Advantus360 (2024) suggests conducting a thorough risk assessment as the foundational step in building an effective information security program. This involves identifying potential risks and vulnerabilities within the organization's IT environment, including hardware, software, and networks. Understanding these risks allows organizations to prioritize resources and focus on the most critical threats to their information assets (Cornes, 2024).

More so, establishing clear and comprehensive security policies and procedures is vital (Exabeam, 2024b). These documents serve as guidelines for employees on how to handle sensitive information and respond to security incidents. Regularly updating these policies ensures they remain relevant in the face of evolving threats and technologies (Mallory, 2020).

Employees are often the weakest link in an organization's security posture. Implementing a user awareness and training program helps educate staff about cyber security best practices, recognizing phishing attempts, and securely handling sensitive information. Ongoing training fosters a culture of security within the organization (Advantus360, 2024).

According to Cornes (2024), implementing strong access controls is crucial to limit who can access sensitive data and systems. This includes role-based access control (RBAC), ensuring that users have access only to the information necessary for their roles. Mallory (2020) supports this by putting much emphasis on regular reviews of access privileges help maintain security as personnel changes occur.

Additionally, employing advanced technologies for threat detection and response is essential for a proactive security posture (Advantus360, 2024). Tools such as intrusion detection systems (IDS), endpoint detection and response (EDR), and security information and event management (SIEM) solutions help organizations identify and respond to threats quickly. An incident response plan should also be in place to guide actions during a security breach.

Furthermore, Holdsworth & Kosinski (2024) asserts that regular monitoring of security measures is critical for maintaining an effective information security program. Continuous auditing helps identify weaknesses or areas for improvement in security practices, ensuring compliance with industry regulations while reinforcing trust with clients and partners.

Ensuring that the information security program complies with relevant laws, regulations, and industry standards is crucial. This includes adhering to frameworks like GDPR, HIPAA, or PCI DSS, which help mitigate legal risks associated with data breaches (Cornes, 2025; Mallory, 2020). Having a well-defined incident response plan is essential for minimizing the impact of security incidents. This plan should outline the steps to take when a breach occurs, including communication strategies, roles of team members, and recovery processes (Mallory 2020, 2024; Exabeam, 2024b).

A robust information security program integrates these key components to create a comprehensive defence against information security threats. By conducting risk assessments, establishing clear policies, training employees, implementing strong access controls, utilizing advanced detection technologies, continuously monitoring systems, ensuring compliance, and preparing for incidents, organizations can significantly enhance their information security posture and protect their critical assets from evolving threats.

5.4 Suggestion for further studies

This research identified significant vulnerabilities in RZM Murowa's information systems, including outdated infrastructure, unlicensed software, weak password management, and a lack of security awareness. Consequently, further investigation is needed to fully assess the impact of improving information security and develop evidence-based practices. While the research identified some promising strategies and technologies, their practical application and implementation require further study. Key areas for future research include:

- **Incident Response Planning:** Exploring best practices for creating effective incident response plans specifically for the mining industry, with an emphasis on rapid recovery and communication during cyberattacks.
- **Emerging Technology:** Investigating the effects of IoT, AI, and automation on mining security, particularly their potential to enhance threat detection and operational resilience.
- **Regulatory Compliance:** Examining the data protection regulations relevant to the mining sector, including frameworks like the Kimberley Process Certification Scheme, to ensure ethical operations and compliance.
- **Zero Trust Security:** Evaluating the implementation of a Zero Trust security model (Never Trust, Always Verify) for modern multi-cloud networks, focusing on enforcing granular security policies for all connections.
- **AI/ML for Cyber threat Mitigation:** Researching the use of AI and machine learning to proactively predict and neutralize cyber threats before they can cause damage.
- **Block-chain Security:** Exploring the potential of block-chain technology to enhance data security through decentralized and immutable data storage.

These are the areas the researcher thinks if they are explored in detail might also help in the enhancement of information security at RZM Murowa. The technologies are not limited to the above named technologies as it is ever evolving.

References

Advantus360. (2024). Your essential cyber risk assement guide. *Advantus360*.

Australia, M. (2022, July 14). *How can mining companies protect their operational technology networks?* Retrieved from mine.nridigital.com: https://mine.nridigital.com/mine_australia_jul22/ar_health_and_safety

Ava), A. &. (n.d.). *End-to-end security solutions*. Retrieved from http://www.avigilon.com/

Bhandari, P. (2023, June 21). *Population vs. sample: Definitions, Differences & Examples*. Retrieved from Scribbr: https://www.scribbr.com/methodology/population-vs-sample/(Bhandari, Population vs.sample: Definitions, Differences & Examples 2023)

Blair, A. (2024, July 16). *Operational Disruption the main cybersecrity threat in mining*. Retrieved from Mining Technology: https://www.mining-technology.com/interviews/operational-disruption-the-main-cybersecurity-threat-in-mining/

Boyce, C. &. (2006). Conducting in-depth Interviews: A Guide for Designing and Conducting In-Depth Interviews. *Pathfinder International Tool Series*.

Chikane, A. &. (2011). *Compliance Verification Report. In KP Monitoring Team.* Retrieved from kimberlyprocess.com: https://www.kimberleyprocess.com/

Cornes, M. (2025). Future proofing cybersecurity insights from a cybersecurity expert. *Digital Journal*.

Cybersecurity/Network and Information Security. (n.d.). Retrieved from Joinup: https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/cybersecurity-network-and-information-security

Exabeam. (2024, July 3). *The 12 elements of an Information Security Policy*. Retrieved from Exabeam.com: https://www.exabeam.com/explainers/information-security/the-12-elements-of-an-information-security-policy/

Exabeam. (2024b, November 5). *What is Information Security (InfoSec)? Goals, types and applications*. Retrieved from exabeam.com: https://www.exabeam.com/explainers/information-security/information-security-goals-types-and-applications/

George, T. (n.d.). What Is an Observational Study?

Holdsworth, J. &. (2024, August 26). *Information Security*. Retrieved from IBM Research: https://www.ibm.com/topics/information-security

IBM. (2024). *Cost of a data breach.* IBM. Retrieved from IBM.COM.

Intelligence, G. T. (2022, June 22). *How can mining companies protect their OT networks?* Retrieved from mining-technology.com: https://www.mining-technology.com/analyst-comment/mining-companies-protect-ot-networks/

Kirenberg, A. M. (2020). A mathematical model of information security for a mining company. E3S Web of Conferences.

Leonida, C. (2022, November). ENGINEERING AND MINING JOURNAL. *Securing-minings-digital-ecosystems*.

Makusheva, G. (2019). Assessment of the Protection and Efficiency of Work of Informatin Systems Used in the Mining Industry. E3S Web of Conferences.

Mallory, P. (2020, September 15). *Time to update your cybersecurity policy*. Retrieved from INFOSEC: https://www.infosecinstitute.com/resources/management-compliance-auditing/time-to-update-your-cybersecurity-policy/

Manav. (2023, October 30). *Securing the Connected Mine: Managing Cyber Risks in Mining's Digital Transformation. Future Bridge Mining.* Retrieved from mining-events.com: https://mining-events.com/securing-the-connected-mine-managing-cyber-risks-in-mining-digital-transformation/

Manav. (2023b, October 30). *Securing the Connected Mine: Managing Cyber Risks in Mining's Digital Transformation*. Retrieved from mining-events.com: https://mining-events.com/securing-the-connected-mine-managing-cyber-risks-in-mining-digital-transformation

Mishchuk, I. S. (2021). Ensuring security of economic and informational interests of mining enterprises taking into account innovative technological trends. *Eastern-European Journal of Enterprise Technologies,2.*, 42-54.

Muechen, R. (2011). *Doing qualitative research.* Retrieved from APA Dictionary of Psychology: https://us.sagepub.com/en-us/nam/qualitative-research/book271731

Nicolas, A. &. (2023, August 29). *Thematic Analysis-A Guide with Examples*. Retrieved from ResearchProspect: https://www.researchprospect.com/thematic-analysis/

Nieles, M. D. (2019). *Introduction to information security.* NIST.

Numaan, H. (2015). *Cyber threats to the Mining Industry.* Retrieved from Trend Micro.

Paulson, D. A. (1997). Social research methods. *Quantitative and qualitative approaches*.

Rapson, K. C. (2024). *Smart Mining Solutions.*

Robinson, P. (2024, November 6). *Top 10 security measures every organization should have.* Retrieved from lepide.com: https://www.lepide.com/blog/top-10-security-measures-every-organization-should-have/

Robinson, S. (2020, October 4). *Interview Sampling by Berverly Peters*. Retrieved from aea365: https://aea365.org/blog/interview-sampling-by-beverly-peters/

Rodrigues, J. (2024, April 2). *Top 5 methods of protecting data*. Retrieved from TitanFile: https://www.titanfile.com/blog/5-methods-of-protecting-data/

Thomas, H. (2011). Social-Technical Systems. *International Journal of Sociotechnology and Knowledge Development*, 2-3.

Tunnicliffe, A. (2024, September 2). *cybersecurity -it-ot-mining*. Retrieved from Mining Technology: https:www.mining-technology.com/features/cybersecurity -it-ot-mining/

visiondci.com. (2024, July 8). *Ensuring safety and stability: Best practices for security in the Mining sector*. Retrieved from visiondci.com: https://visiondci.com/ensuring-safety-and-stability-best-practices-for-security-in-the-mining-sector/

Works, C. (2024, June 10). *Cybersecurity in mining industry*. Retrieved from commit.works: https://www.commit.works/cybersecurity

Appendices

Informed consent

My name is Rumbidzai, a fourth year Computer Science student from Africa University. I am kindly asking you to participate in this study by filling in the questionnaire or participating in a short interview.

The purpose of the study is to analyse and assess the existing information security infrastructure, technologies and strategies in order to find areas that need improvement. The study aims to reach 40 participants.

If you decide to participate, you will answer questions or participate in the interview. It is expected that this will take about 10 minutes at minimum.

There is no harm or risk whatsoever expected from this practice. The research aims to find strategies and technologies that can be used at RZM Murowa mine to improve information security and reduce the chances of the system being compromised.

No personal detail or name of the participant shall be disclosed to anyone unless one is willing to let it be disclosed. Sensitive information will be confidential and treated with secrecy.

Participation in this study is voluntary. If a participant decides not to participate in this study, their decision will not harm any relationship.

If they chose to participate, they are free to withdraw their consent and discontinue participation without penalty.

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

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

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

Name of Research Participant (please print) Date

Signature of Research Participant or legally authorised representative

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

Name of Researcher: Rumbidzai Chakumarani

Interview Questions

Basic demographic information

1. Name (Optional): □

2. Role at RZM Murowa: □

3. Department: □

Understanding the Current Information Security Landscape

1. What do you understand about information security in general?
2. What are the information security measures in place at RZM Murowa?
3. What are the primary information security challenges faced by RZM Murowa?
4. How would you rate the overall information security posture of the company?
5. How frequent do you have information security awareness campaigns?
6. How can security awareness be enhanced among employees? 8. What security incident have you witnessed at RZM Murowa?
7. In your own opinion, how important is information security to the organization (RZM Murowa)?
8. What challenges have you encountered with compliance to security procedures and policies in your daily work?

9. How effective are the current information security measures and technologies helping you perform your job securely?
10. How do you report a security incident without fear of the repercussions associated with it?
11. What are your biggest concerns regarding information security at RZM Murowa.
12. What strategies and technologies that you think can be incorporated to enhance the already existing information security at RZM Murowa?
13. Is the management involved in information security decision-making process?
14. What plans are there in line with information security infrastructural development?
15. Is there anything else you would like to add about information security at RZM Murowa?

Observation Guide

Purpose: To observe and evaluate the information security practices and controls within RZM Murowa.

Scope: This guide covers the observation of physical security, data security, network security, user behaviour, incident response and compliance.

Methodology: Participant observation on-site.

Observation Area	Observation Notes	Recommendations
Physical Security	• Access controls(ID Cards Biometrics	Recommend specific actions to improve physical security, such as upgrading access

	• Perimeter security • CCTV surveillance • Secure Storage of sensitive equipment • Asset Labelling & Tracking	controls or increasing CCTV coverage.
Network Security	• Intrusion Detection/prevention systems • Network segmentation(VLANs) • Firewall configuration	Recommend specific actions to enhance network security, such as implementing stronger firewall rules or deploying additional security tools
Data Security	• Data classification • Data encryption • Regular backups • Secure Data Transmission(HTTPs, SFTP) • Access controls(role-based) • Recovery practices	Recommend specific actions to improve data security, such as enforcing stricter data classification policies or implementing stronger encryption
User Behaviour	• Security awareness training programs,	Recommend specific actions to improve user awareness

	- Phishing simulations - Strong password policies. - Incident Reporting Procedures	and training, such as conducting more frequent training sessions or implementing stronger password policies.
Incident Response	- Incident response plan documented - Incident Response Team Trained. - Incident reporting procedures investigation processes.	Recommend specific actions to improve incident response, such as updating the incident response plan or conducting regular table top exercises.
Compliance	- Regulatory compliance - Industry security standards adopted - Regular Compliance audits	

AFRICA UNIVERSITY®
A United Methodist-Related Institution

COLLEGE OF ENGINEERING AND APPLIED SCIENCES

29/05/2024

Africa University Research Ethics Committee

Ref: Approval for AUREC Proposal Submission

Rumbidzai Chakumarani has worked on the proposal and I can confirm that it is ready for review by your esteemed committee.

Respectfully submitted,

LOVELY T TEMBANI-FUNDISI

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

Supervisor’s Name Supervisor’s Signature

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

H.O.D’s Name H.O.D’s Signature

Murowa Diamonds Mine

Research Approval Form

Project Title: Enhancing Information Security at RZM Murowa: strategies, technologies and recommendations.

Researcher Information:

Name: Rumbidzai Chakumarani

Affiliation: Africa University, College of Engineering and Applied Sciences

Contact Details:

- Email: chakumaranir@africau.edu
- Phone: +263 783106126

Project Description:

This research project aims to investigate the current information security system, strategies and technologies at Murowa Diamonds Mine, striving to find areas that need improvement, new technologies and strategies that could be adapted to enhance the information security. The research will involve the following activities:

1. Interviews with key personnel, including Information Officers and system users to understand the existing information security system so as to find areas that need improvement and any strategies that would improve it.

2. Review of relevant documentation, such as IT security policies, data backup and recovery procedures, and incident response plans.
3. Analysis of the current IT infrastructure, including servers, storage systems, and network configurations, to assess the level of data protection and security measures in place.
4. Evaluation of data governance practices, including, access controls, and monitoring mechanisms.
5. Benchmarking of Murowa Diamonds Mine's data management and security practices against industry best practices and standards.
6. Development of a comprehensive case study report detailing the findings, recommendations, and a roadmap for improving information security at RZM Murowa Diamonds Mine.

The research project is expected to be completed within 6 months, and the final report will be shared with the Murowa Diamonds Mine management team.

Project Timeline

Page 1 of 2

Effective Date: 01/03/2021 Version Number: 0 Document No: HRA/JQ50/FOR/029

The approval is granted, and Murowa Diamonds Mine will provide the necessary access, resources, and support to facilitate the research project.

Start Date: 2024/06/20 End Date: 2025/03/31

Researcher

IS&T Attaché, Murowa Diamonds Mine:

Name: Rumbidzai Chakumarani Signature: ……………………………….. Date: 2024/06/24

Approved By

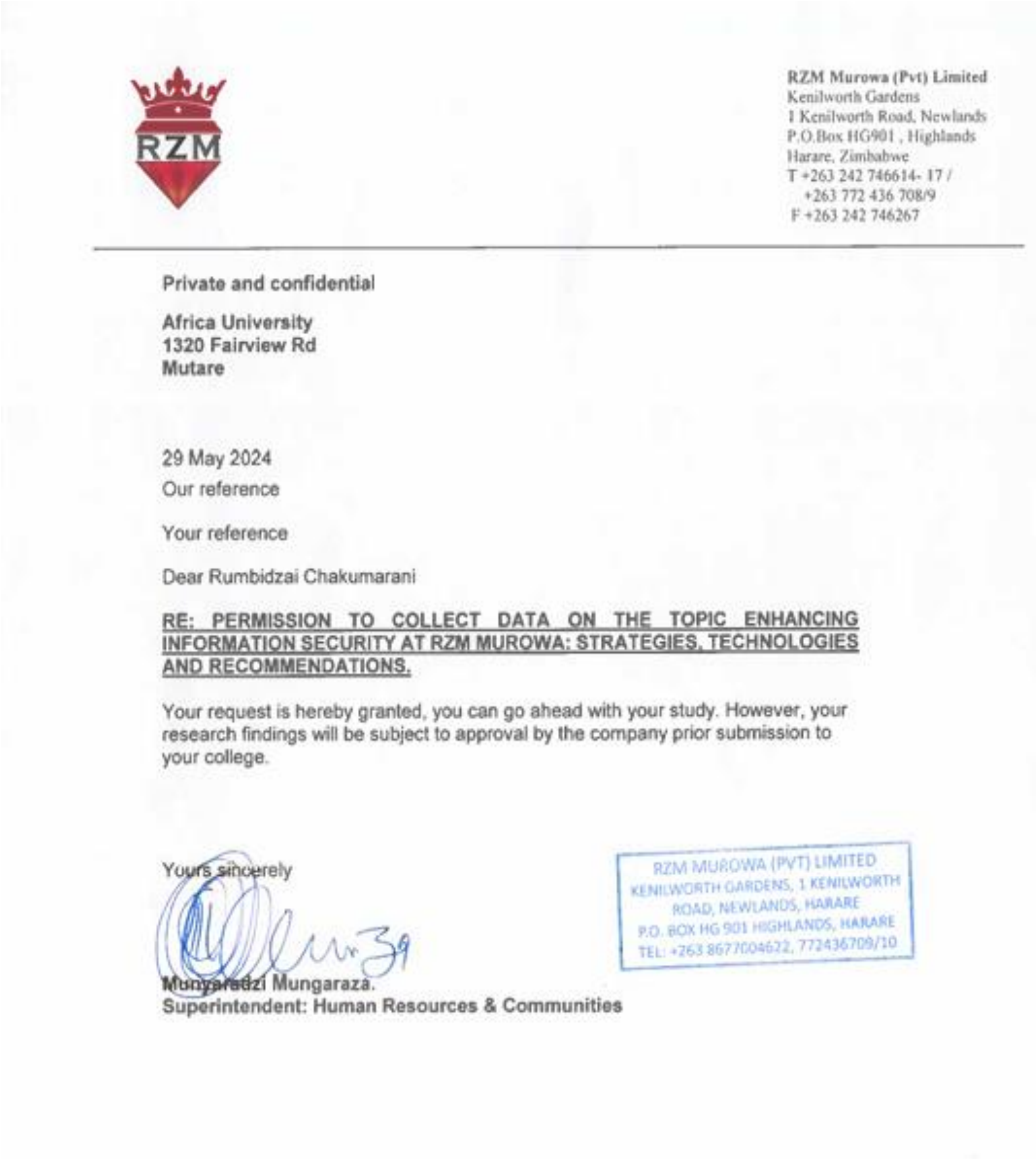
IS&T Officer, Murowa Diamonds Mine:

Name: Rumbidzai Chimwanda Signature: ……Rhims Date: 2024/06/05

Page 2 of 2

Effective Date: 01/03/2021 Version Number: 0 Document No: HRA/JQ50/FOR/029

The approval is granted, and Murowa Diamonds Mine will provide the necessary access, resources, and support to facilitate the research project.



RZM

RZM Murowa (Pvt) Limited
Kenilworth Gardens
1 Kenilworth Road, Newlands
P.O.Box HG901 , Highlands
Harare, Zimbabwe
T +263 242 746614- 17 /
+263 772 436 708/9
F +263 242 746267

Private and confidential

Africa University
1320 Fairview Rd
Mutare

29 May 2024

Our reference

Your reference

Dear Rumbidzai Chakumarani

RE: PERMISSION TO COLLECT DATA ON THE TOPIC ENHANCING INFORMATION SECURITY AT RZM MUROWA: STRATEGIES, TECHNOLOGIES AND RECOMMENDATIONS.

Your request is hereby granted, you can go ahead with your study. However, your research findings will be subject to approval by the company prior submission to your college.

Yours sincerely

RZM MUROWA (PVT) LIMITED
KENILWORTH GARDENS, 1 KENILWORTH
ROAD, NEWLANDS, HARARE
P.O. BOX HG 901 HIGHLANDS, HARARE
TEL: +263 8677004622, 772436709/10

Munyaradzi Mungaraza.
Superintendent: Human Resources & Communities

AFRICA UNIVERSITY

(A United Methodist-Related Institution)

For office use only

Protocol no. ………………….

Type of review: Full Committee □

Expedited □

Exempted □

Office stamp

Fees paid/receipt number: ………………..

AFRICA UNIVERSITYRESEARCH ETHICS COMMITTEE (AUREC)

APPLICATION FOR INITIAL REVIEW

NB: This form must be completed by all persons/teams applying for ethical review by AUREC. Upon completion by the investigator(s) /researcher(s) it should be submitted electronically to AUREC, Africa University, Fairfield Road, Old Mutare, P.O. Box 1320, Mutare. Application fees (to cover the costs of reviewing proposal) should be paid to the Africa University Business Office, and proof of payment should accompany each application. Please complete all sections of this application form. If there is insufficient space on the form you may use additional pages. Check list

This checklist is meant to aid researchers in preparing a complete application package and to help expedite review by the AUREC. Please tick all boxes as appropriate (Indicate **N/A** where inapplicable).

CONTACT PERSON'S NAME: RUMBIDZAI CHAKUMARANI

CONTACT ADDRESS: 171 Shishdale, Murehwa

____

chakumaranir@africau.edu

EMAIL ADDRESS: +263783106126

CONTACT NO:

Undergraduates

		Applicant	**AUREC**
1	Application form duly completed	√	

2	Electronic version of research proposal to aurec@africau.edu	√	
3	Consent forms in English and local language of study population	√	
4	Advertisement or letter or card used for recruiting participants and any supplementary information *(if applicable).*	N/A	
5	Data collection tools being administered during the study in English and local language of study population *(if applicable)* included in the proposal	√	
6	Budget and timeframe included in the proposal.	√	
7	Approval letter from your academic supervisor/college or institution	√	
8	Approval letter from authorities where study will be conducted	√	
9	Application fee paid at AU Business Office and receipt (or copy) attached to application form.	√	

Post graduates and other researchers

		Applicant	**AUREC**
1	Application form duly completed		
2	Electronic version of full research proposal (chapter 1 – 3 completed) to aurec@africau.edu		
3	Proposal summary (see guidelines below)		
4	Consent form in English and local language of study population		
5	Advertisement or letter or card used for recruiting participants and any supplementary information *(if applicable).*		

6	Data collection tools being administered during the study in English and local language of study population (if applicable)		
7	Budget and timeframe		
8	Approval letter from academic supervisor/college or institution *(if you are a student)*		
9	Approval letter from authorities where study will be conducted		
10	Application fee paid at AU Business Office and receipt attached to application form.		
12	CV’s for D Phil and Phd candidates.		

Rumbidzai Chakumarani 31 /05/ 24

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

Signature: Investigator/Researcher Name Date

1. General information

1.1. Study title: Enhancing information security at RZM Murowa: strategies, technologies and recommendations.

1.2. Name of Principal

Investigator (PI)/Researcher: Rumbidzai Chakumarani

1.3. Nationality of

Investigator/Researcher: Zimbabwean

1.4. Proposed date of start of study: June 2024

1.5. Expected duration of study: 12 Months

1.6. Study site(s) in

Zimbabwe: RZM Murowa, Zvishavane

1.7. Sites outside Zimbabwe: None

1.8. Study budget:____$70 USD__________Source of Funding: _____Self______

1.9. Is the researcher a student? Yes

1.10. If Yes, indicate the following:

1.10.1. Name and address of institution: Africa University 1320, Fairview Road, Mutare.

1.10.2. College: Engineering and Applied Sciences

1.10.3. Level of study Undergraduate/Master's/PhD : Undergraduate

1.10.4. Name of Supervisor: LTembani-Fundis

1.11. If No to question 1.10, then indicate the following:

1.11.1. Name and address of institution: ____

1.11.2. Academic Title of PI: ____

1.11.3. ExistingQualifications: ____

1.11.4. 1.11.4. Co Investigators:

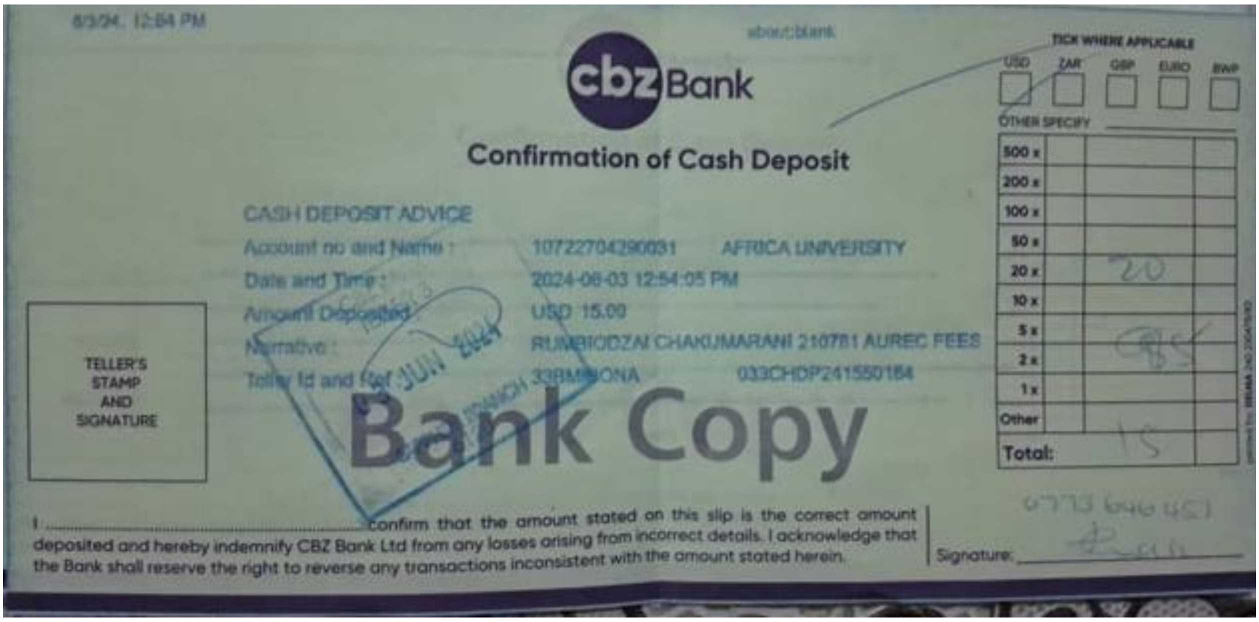
Names:	Qualifications	Institution

2. Statement by the investigator

I Rumbidzai Chakumarani certify that the information in this application document and the accompanying documents is true and complete in all respects. I confirm that the application has NOT been rejected by any other ethics review committee.

Signature ________________________ Date: 31 /05/ 24

AUREC Fees



8/3/24, 12:54 PM

about:blank

cbz Bank

Confirmation of Cash Deposit

CASH DEPOSIT ADVICE

Account no and Name : 10722704290031 AFRICA UNIVERSITY

Date and Time : 2024-08-03 12:54:05 PM

Amount Deposited : USD 15.00

Narrative : RUMBIDZAI CHAKUMARANI 210781 AUREC FEES

Teller Id and Ref : 33BMBONA 033CHDP241550184

JUN 2024

BRANCH

Bank Copy

TELLER'S STAMP AND SIGNATURE

TICK WHERE APPLICABLE

USD □ ZAR □ GBP □ EURO □ BWP □

OTHER SPECIFY ____________

500 x			
200 x			
100 x			
50 x			
20 x		20	
10 x			
5 x		[illegible]	
2 x			
1 x			
Other			
Total:		15	

I .... confirm that the amount stated on this slip is the correct amount deposited and hereby indemnify CBZ Bank Ltd from any losses arising from incorrect details. I acknowledge that the Bank shall reserve the right to reverse any transactions inconsistent with the amount stated herein.

0773 646 451

Signature: ____________

Application for Initial Review Form, Version October 2021

AFRICA UNIVERSITY
A United Methodist-Related Institution

"Investing in Africa's future"

AFRICA UNIVERSITY RESEARCH ETHICS COMMITTEE (AUREC)

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

Ref: AU 3403/24

6 August, 2024

Rumbidzai Chakumarani
C/O Africa University
Box 1320
MUTARE

RE: **ENHANCING INFORMATION SECURITY AT RZM MUROWA: STRATEGIES, TECHNOLOGIES AND RECOMMENDATIONS**

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

The approval is based on the following.
a) Research proposal

- **APPROVAL NUMBER** AUREC 3403/24

This number should be used on all correspondences, consent forms, and appropriate documents.

- **AUREC MEETING DATE** NA
- **APPROVAL DATE** August 6, 2024
- **EXPIRATION DATE** August 6, 2025
- **TYPE OF MEETING**: Expedited
  After the expiration date, this research may only continue upon renewal. A progress report on a standard AUREC form should be submitted a month before the expiration date for renewal purposes.
- **SERIOUS ADVERSE EVENTS** All serious problems concerning subject safety must be reported to AUREC within 3 working days on the standard AUREC form.
- **MODIFICATIONS** Prior AUREC approval is required before implementing any changes in the proposal (including changes in the consent documents)
- **TERMINATION OF STUDY** Upon termination of the study a report has to be submitted to

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

AUREC. **Yours Faithfully**

Chinzou

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