Bindura University of Science Education



FACULTY OF SCIENCE AND ENGINEERING
DEPARTMENT OF COMPUTER SCIENCE

ENHANCING CYBERSECURITY STRATEGIES IN PRIVATE FIRMS: A CASE STUDY OF LOCAL PRIVATE COMPANIES IN ZIMBABWE (PVT)

DIMBA ALFRED KUDZANAI

B222903B

PROGRAME: NETWORK ENGINEERING

SUPERVISOR: MR CHITUMA

DECLARATION

I, Dimba Alfred Kudzanai hereby declare that the dissertation titled: **"Analysis of Cybersecurity Vulnerabilities and Development of a Cybersecurity Strategy for Private Companies in Zimbabwe (PVT)"**is my original work and has not been submitted for a degree at Bindura University.

I confirm that all sources used or quoted have been acknowledged through full referencing and citation. This research was conducted ethically, and all information obtained from participants was treated with confidentiality.

ACKNOWLEDGEMENT

I would like to acknowledge my Father in Heaven, Almighty God who allows all things to work together for our good. I would like to express my sincere gratitude to God Almighty for the wisdom, strength, and perseverance that enabled me to complete this study. I extend my heartfelt appreciation to my supervisor, Mr. Chituma, for the guidance, constructive criticism, and continuous support throughout the research process. I am also grateful to all respondents who participated in this study for their time and valuable insights. Special thanks go to my family and friends for their encouragement and support during this academic journey.

ABSTRACT

Cybersecurity has become a critical concern for organizations as dependency on computer systems and digital communication increases. Small and medium-sized enterprises (SMEs) are particularly vulnerable due to limited financial and technical resources to implement robust cybersecurity frameworks. A mixed-method research design was employed, involving questionnaires, observations, and document analysis. Data was collected from employees, management, and ICT personnel. The study assessed cybersecurity awareness levels, identified vulnerabilities within digital systems, and evaluated the applicability of cybersecurity frameworks such as ISO 27001 and NIST. Results revealed that employee cybersecurity awareness is low, cybersecurity policies are either informal or nonexistent, and system vulnerabilities are not monitored periodically. The study concludes that simple, low-cost cybersecurity measures including staff training, strong password policies, network access control, and adoption of selected components of ISO 27001 and NIST can significantly improve the organization's security posture. The study recommends the development of a cybersecurity policy, continuous awareness training, periodic vulnerability assessments, and implementation of a structured cybersecurity framework.

Contents

DECLARATION ..... **i**

ACKNOWLEDGEMENT ..... **ii**

ABSTRACT ..... **iii**

CHAPTER 1 ..... **1**

PROBLEM IDENTIFICATION **1**

1.1 INTRODUCTION **1**

1.2 BACKGROUND TO THE STUDY **2**

1.3 PROBLEM STATEMENT **4**

1.4 RESEARCH OBJECTIVES **6**

1.5 RESEARCH QUESTIONS **6**

1.6 JUSTIFICATION / SIGNIFICANCE OF THE STUDY **7**

1.7 ASSUMPTIONS OF THE STUDY **9**

1.8 LIMITATIONS / CHALLENGES OF THE STUDY **10**

1.9 SCOPE / DELIMITATION OF THE RESEARCH **11**

1.10 DEFINITION OF TERMS **13**

1.11 SUMMARY **15**

CHAPTER 2 ..... **16**

LITERATURE REVIEW **16**

2.1 INTRODUCTION **16**

2.2 CONCEPTUAL FRAMEWORK **16**

2.3 THEORETICAL FRAMEWORK **18**

2.4 EMPIRICAL AND THEORETICAL LITERATURE **20**

2.5 RESEARCH GAP ANALYSIS **28**

2.6 SUMMARY **29**

CHAPTER 3 ..... **30**

RESEARCH METHODOLOGY **30**

3.1 INTRODUCTION **30**

3.2 RESEARCH DESIGN **30**

3.3 POPULATION AND SAMPLE **31**

3.4 RESEARCH INSTRUMENTS **33**

3.5 RELIABILITY AND VALIDITY **35**

3.6 DATA COLLECTION PROCESS **35**

3.7 ETHICAL CONSIDERATIONS **36**

3.8 SYSTEM DOCUMENTATION **37**

3.9 SYSTEM DEVELOPMENT **39**

3.10 SYSTEM ANALYSIS **41**

3.11 SYSTEM DESIGN **43**

3.12 CODING **44**

3.13 IMPLEMENTATION **44**

3.14 SUMMARY **45**

CHAPTER 4 ..... **46**

DATA PRESENTATION, ANALYSIS AND INTERPRETATION **46**

4.1 INTRODUCTION **46**

4.2 DEMOGRAPHIC INFORMATION OF RESPONDENTS **46**

4.3 CYBERSECURITY AWARENESS LEVELS **48**

4.4 IDENTIFIED CYBERSECURITY VULNERABILITIES **50**

4.5 ADEQUACY OF EXISTING CYBERSECURITY MEASURES **52**

4.6 CYBERSECURITY RISKS FACING THE ORGANISATION **53**

4.7 CHALLENGES IN IMPLEMENTING THE SYSTEM **55**

4.8 SYSTEM TESTING AND VALIDATION **56**

4.9 SUMMARY **59**

CHAPTER 5 ..... **60**

CONCLUSIONS AND RECOMMENDATIONS **60**

5.1 INTRODUCTION **60**

5.2 MAJOR CONCLUSIONS DRAWN **61**

5.3 RECOMMENDATIONS **63**

5.4 SUMMARY **65**

REFERENCE LIST **66**

LIST OF TABLES

Table 1Hardware Requirements _____ **38**

Table 2: Software Requirements _____ **39**

Table 3: System Development Tools _____ **40**

Table 4: System Analysis _____ **41**

Table 5: Demographic Characteristics of Respondents _____ **47**

Table 6: Employee Cybersecurity Awareness Levels _____ **49**

Table 7: Identified Cybersecurity Vulnerabilities _____ **51**

Table 8: Comparison with ISO 27001 and NIST _____ **52**

Table 9: Identified Cybersecurity Risks _____ **54**

Table 10: Challenges in Cybersecurity Implementation _____ **56**

Table 11: White Box Testing _____ **59**

LIST OF FIGURES

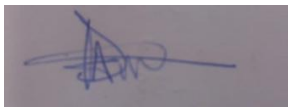
Figure 1 Coding Snipet **44**
Figure 2 Gender Distribution Pie Chart **49**
Figure 3 ICMS Dashboard **59**
Figure 4 Cybersecurity Training Modules Page **60**
Figure 5 Email Scanner Page **60**
Figure 6 Security Incidents Page **61**
Figure 7 Scanned Email Results Page **61**
Figure 8 Phishing Simulation Page **62**

DISSERTATION APPROVAL FORM

Name: **Dimba Alfred Kudzanai**

Student Number: **B222903B**

Dissertation Title: **Enhancing cyber security strategies in private firms "A case study of local private companies in Zimbabwe (pvt)"**

Signature 

APPROVALS

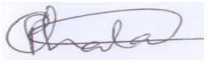
SUPERVISOR

Name: **Mr Chituma**

Signature: 

CHAIRPERSON

Name:_ **Mr Chaka**

Signature: 



CHAPTER 1
PROBLEM IDENTIFICATION

1.1 INTRODUCTION

The rapid growth of digital technologies has transformed how organizations operate and compete in the modern business environment. Almost every industry, including engineering, now relies on computer systems, internet connectivity, cloud storage platforms, and digital communication tools to improve efficiency, enhance decision-making, and support daily operations (Smith, 2022). Although digital transformation brings convenience and productivity gains, it also introduces new risks, particularly related to cybersecurity. Cybersecurity refers to the protection of digital systems, networks, and data from unauthorized access, disruption, or damage caused by internal or external threats (Stallings and Brown, 2018).

Globally, cyberattacks are increasing in frequency, complexity, and financial impact. Reports from international cybersecurity agencies indicate that small and medium enterprises (SMEs) are the most targeted because they often lack adequate security systems, cybersecurity expertise, and formal security policies (Verizon, 2024). Unlike large corporations with dedicated cybersecurity departments, SMEs usually invest minimally in cybersecurity, assuming they are unlikely to be targeted. This misconception makes them easy targets for hackers (Furnell and Clarke, 2020). Cybercriminals often exploit weak passwords, unpatched software, unsecured networks, social engineering attacks, and a lack of employee awareness to gain unauthorized access to company data (Hadnagy, 2018).

In the context of developing countries like Zimbabwe, cybersecurity challenges are intensified by limited financial resources, a lack of skilled IT personnel, and limited awareness among employees (Moyo and Sibanda, 2021). Engineering companies store sensitive information, including project documentation, technical designs, client contracts, supplier databases, and confidential business strategies. If this information falls into the wrong hands, the organization may incur financial losses, operational disruptions, reputational damage, and legal consequences (Von Solms and Van Niekerk, 2013).

This study, therefore, investigates cybersecurity vulnerabilities at the organizations and develops the Integrated Cybersecurity Management System (ICMS), a practical and cost-

effective solution incorporating training modules, policy management, incident reporting, and phishing simulation capabilities, tailored to the operational needs of the organization.

1.2 BACKGROUND TO THE STUDY

1.2.1 Profile of the Case Study Organization

The research was conducted through data collected from ten (10) Information Technology students who were on industrial internship at different private firms across Zimbabwe during the 2023-2024 academic period. These students were classmates of the researcher and were drawn from the same academic program. Each student was placed at a different organization for at least 3 months, during which they gained firsthand exposure to the organization's ICT infrastructure, security practices, and operational challenges.

The host organizations where the students were attached represent a diverse cross-section of Zimbabwe's private sector. The breakdown of host organizations is as follows:

Three (3) engineering and construction firms – These organizations handle sensitive project documentation, technical designs, and client contracts. They rely heavily on specialized engineering software and maintain both office-based and site-based IT systems.

Two (2) financial services companies – These organizations process sensitive financial transactions and client data. They are subject to regulatory requirements under Zimbabwe's Cyber and Data Protection Act and handle high-value digital assets.

Two (2) manufacturing enterprises – These organizations manage supply chains, production schedules, and inventory systems. Their operations combine traditional IT systems with operational technology for production control.

Two (2) retail and distribution companies – These organizations process customer data, manage e-commerce platforms, and handle payment processing systems. They face threats related to point-of-sale systems and customer data protection.

One (1) telecommunications service provider – This organization manages network infrastructure and customer communication systems, facing advanced persistent threats due to its role in the communications sector.

The host organizations range in size from small enterprises with approximately 15 employees

to medium-sized firms with up to 120 employees. Collectively, these organizations employ an estimated 450 people across all sectors. The diversity of sectors, sizes, and operational contexts provides a comprehensive view of cybersecurity challenges facing private firms in Zimbabwe.

For confidentiality purposes and in accordance with ethical research principles (Creswell and Creswell, 2018), individual organizations are not named in this study. Student respondents are identified by codes (S1 through S10) to protect their identities and those of their host organizations. The students' host organizations were informed of the research and provided consent for their internship students to participate in data collection activities.

1.2.2 Cybersecurity Landscape in Zimbabwe

In the modern digital landscape, cybersecurity has become a critical concern for organizations worldwide, particularly SMEs that often operate with limited budgets and technical expertise (Anderson, 2021). According to research, SMEs face an evolving range of threats, from phishing and data breaches to ransomware and system sabotage (Chikwanha, 2023). During the researcher's internship, it was discovered that the organization is vulnerable to cybersecurity breaches due to legacy systems, limited security budgets, and low awareness of cybersecurity best practices. The increasing digitization of operations, including emails, databases, and cloud platforms, while improving efficiency, has simultaneously expanded the organization's exposure to cyber threats.

1.2.3 Zimbabwean Government Cybersecurity Initiatives

The Government of Zimbabwe has taken significant steps to address cybersecurity challenges in recent years. In 2018, the Government enacted the **Cyber and Data Protection Act [Chapter 12:07]** (Government of Zimbabwe, 2018), which provides a legal framework for cybersecurity and data protection in the country. The Act establishes the Cyber Security Center and outlines offenses related to cybercrime, including unauthorized access, data interception, and system interference (Mandizha and Chirume, 2021).

In 2021, the Government launched the **National Cybersecurity Awareness Campaign** to educate citizens and businesses about online safety and cyber threats (Potraz, 2021). The Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) has been instrumental in implementing these awareness programs across all provinces (POTRAZ, 2023).

Furthermore, Zimbabwe is a signatory to the **African Union Convention on Cyber Security and Personal Data Protection** (African Union, 2020), demonstrating its commitment to regional cooperation in combating cybercrime. The Government has also established the **Computer Emergency Response Team (CERT)** to coordinate incident response and provide cybersecurity guidance to organizations (CERT Zimbabwe, 2024).

Despite these efforts, implementation challenges remain, particularly for SMEs, which often struggle to comply with regulatory requirements due to resource constraints (Moyo and Sibanda, 2021). The gap between policy and practice continues to expose organizations to cyber threats.

This background highlights the urgent need for a structured cybersecurity strategy to protect business operations, client data, and the organization's reputation in an increasingly digital and interconnected industrial environment.

1.3 PROBLEM STATEMENT

Through structured discussions with the ten IT students during their industrial internship period, a pattern of cybersecurity challenges emerged across their respective host organizations. The students reported observing various cybersecurity incidents during their internship, including unauthorized access to confidential company data, website defacement, attempted breaches of internal systems, ransomware infections, and successful phishing attacks. In several cases, the students witness operational disruptions caused by cybersecurity threats, including system downtime lasting several days, delayed project deliveries, and temporary loss of access to critical business platforms. From observations and incident reports, it is evident that cybersecurity threats have negatively affected company operations, project delivery timelines, and overall client confidence across multiple firms in Zimbabwe.

According to the data gathered, several host organizations incurred substantial unplanned expenses related to cybersecurity incidents. These costs included forensic investigations to determine the origins of the breach, system recovery and data restoration, website reconstruction following defacement, and temporary outsourcing of specialized IT support. One engineering firm reportedly incurred over US$18,000 in costs for data recovery and system upgrades following a ransomware incident that encrypted critical design files. Another financial services company incurred penalties for delayed service delivery after its online banking

platform was compromised. Across the ten organizations, the students estimated that cybersecurity incidents resulted in an average 25-40% decline in operational efficiency during

recovery periods, with some organizations losing client contracts due to reputational damage from service interruptions.

The gathered data indicated that most organizations lack comprehensive cybersecurity strategies.

Eight (8) of the ten organizations had no documented formal cybersecurity policy.

Nine (9) organizations had never conducted cybersecurity awareness training for employees.

Seven (7) organizations relied on outdated or unsupported software systems

Ten (10) organizations had no incident response plan in place

Six (6) organizations did not perform regular data backups

Eight (8) organizations lacked basic access controls, such as multi-factor authentication

Employees across these organizations were observed using weak passwords, sharing login credentials, accessing unsecured Wi-Fi networks, and handling sensitive data without adequate protective measures. These observations align with Chikwanha's (2023) findings that Zimbabwean SMEs often lack cybersecurity awareness and formal controls.

i. Without immediate and strategic interventions, the private sector in Zimbabwe faces escalating risks of more severe cyber-attacks, which could result in:

ii. Loss of confidential client and business data (CERT Zimbabwe, 2024)

iii. Significant operational downtime affecting business continuity

iv. Financial losses from system interruptions, ransom payments, and regulatory penalties under the Cyber and Data Protection Act (Government of Zimbabwe, 2018)

v. Permanent damage to the company's reputation, reducing client confidence and competitive positioning

vi. Potential closure of SMEs that cannot recover from major security incidents

Furthermore, the organizations represented in this study fall into what Furnell and Clarke (2020) describe as the "cybersecurity gap." They are too large to rely solely on simple security practices but too small to afford dedicated cybersecurity teams and enterprise-grade security tools. This gap, combined with limited awareness and weak internal controls across the sector, underscores the need for a structured research effort to analyze current vulnerabilities and propose feasible, cost-effective solutions tailored to the resource constraints of private firms in Zimbabwe.

1.4 RESEARCH OBJECTIVES

The study seeks to archive the following questions:

i. To identify the cybersecurity vulnerabilities affecting private firms in Zimbabwe.

ii. To assess the adequacy of current cybersecurity measures used by private firms against the ISO 27001 and NIST frameworks.

iii. To determine the major cybersecurity risks that expose private organizations to operational threats.

iv. To develop a practical and cost-effective cybersecurity solution for private firms in Zimbabwe, specifically a web-based Integrated Cybersecurity Management System (ICMS) incorporating training modules, policy management, incident reporting, and phishing simulation capabilities.

1.5 RESEARCH QUESTIONS

The study seeks to answer the following questions:

i. What cybersecurity vulnerabilities affect organizations in Zimbabwe?

ii. How adequate are the current cybersecurity measures used by organizations in Zimbabwe, benchmarking with frameworks such as ISO 27001 and NIST?

iii. What are the major cybersecurity risks that expose the organization to operational and information-security threats?

iv. What practical and cost-effective cybersecurity solution can be developed for the organizations?

1.6 JUSTIFICATION / SIGNIFICANCE OF THE STUDY

The organizations are currently facing cybersecurity vulnerabilities due to the absence of a formal cybersecurity strategy, limited employee awareness, and inadequate control mechanisms. This study is significant because it provides a practical and affordable pathway for strengthening cybersecurity within the organization.

The significance of this study is outlined under the following key dimensions:

1.6.1 Organizational Significance

The research will directly benefit the organizations by:

i. Identifying existing cybersecurity vulnerabilities within their ICT environment (NIST, 2021)

ii. Providing a structured cybersecurity strategy tailored to the organization's level of resources and maturity

iii. Reducing risks of cyberattacks that may lead to data loss, financial loss, and reputation damage

iv. Enhancing operational continuity by minimizing system downtime caused by cybersecurity incidents

v. Ensuring compliance with Zimbabwe's Cyber and Data Protection Act (Government of Zimbabwe, 2018)

A more secure ICT environment supports efficiency and protects organizational assets, giving the organizations a competitive advantage in the engineering industry.

1.6.2 Contribution to the Engineering and SME Sector

Most small and medium enterprises (SMEs) in Zimbabwe and similar developing economies operate without formal cybersecurity strategies due to limited financial and technical resources (Moyo and Sibanda, 2021). This research contributes to the sector by demonstrating that effective cybersecurity does not always require expensive tools. It presents a practical cybersecurity framework that other engineering-based SMEs can adopt and supports the Government's national cybersecurity awareness objectives (POTRAZ, 2023). The findings will therefore serve as a reference model for other companies experiencing similar challenges.

1.6.3 Academic Significance

This research contributes to existing academic knowledge by:

i. Bridging the literature gap on cybersecurity implementation in engineering SMEs in developing countries
ii. Providing empirical evidence on the relationship between employee awareness, cybersecurity frameworks, and vulnerability levels
iii. Expanding understanding of how ISO 27001 and NIST frameworks can be scaled down to suit SMEs with limited resources (Chen and Zhao, 2021)

Future researchers may build upon this framework to conduct deeper studies in other industries or regions.

1.6.4 Significance to Employees

Employees are often the weakest link in cybersecurity (Hadnagy, 2018). This research helps to:

i. Improve employee knowledge and awareness of cybersecurity best practices
ii. Reduce accidental behaviors that expose the organization to cyber risks (e.g., weak

passwords, negligence, phishing email responses)

iii. Encourage the development of a cybersecurity-conscious culture within the organization

With empowered employees, cybersecurity becomes a shared responsibility rather than an IT-only activity.

1.6.5 Policy and Regulatory Significance

The findings may assist policymakers, government ICT authorities, and industry regulators to:

i. Understand cybersecurity challenges faced by SMEs (Mandizha and Chirume, 2021)

ii. Develop guidelines, training programs, or sector-specific cybersecurity compliance requirements

iii. Enhance the implementation of the Cyber and Data Protection Act (Government of Zimbabwe, 2018)

iv. Support the work of CERT Zimbabwe in incident response coordination (CERT Zimbabwe, 2024)

1.6.6 Economic and Strategic Significance

Cyberattacks can lead to financial loss, business interruption, and loss of clients (Ponemon Institute, 2023). By implementing the recommendations from this study, the organization is likely to:

i. Reduce costs associated with cybersecurity breaches

ii. Protect proprietary and client information, thereby retaining customer trust

iii. Improve business resilience and competitiveness

1.7 ASSUMPTIONS OF THE STUDY

Every research study is based on certain assumptions that must hold for the results to be valid and meaningful (Kothari, 2019). For this study, the following assumptions were made:

1.7.1 Participants Will Provide Honest and Accurate Information: It is assumed that employees, management, and IT personnel at the organizations will respond truthfully during questionnaire completion and interviews. The accuracy of the research findings depends on participants' willingness to disclose real challenges, incidents, and behaviors relating to cybersecurity practices.

1.7.2 Management Will Grant Access to Relevant Documents and Information: The study assumes that the organization will grant access to non-confidential documents such as policies, incident logs, and ICT usage guidelines. Since document analysis forms part of the research methodology, access to these materials is essential.

1.7.3 Participants Understand the Importance of Cybersecurity: It is assumed that employees have at least a basic understanding of ICT usage and awareness of cybersecurity threats, enabling them to respond to the research instruments meaningfully.

1.7.4 There Has Been At Least One Cybersecurity Incident: The study assumes that cybersecurity breaches or suspicious events have occurred at the organizations, aligning with the reports observed during the internship period. This assumption enables assessment of how previous incidents were handled and what lessons were learned.

1.7.5 The ICT Environment Will Remain Operational During the Study: It is assumed that the organization's systems and digital environment will be functional throughout the research period, allowing data to be collected regarding normal cybersecurity practices and system usage.

1.7.6 Respondents Have Access to ICT Tools: It is assumed that respondents (employees and IT personnel) have access to computers, the internet, or internal networks, making it possible to answer questions related to cybersecurity processes and practices.

1.8 LIMITATIONS / CHALLENGES OF THE STUDY

Although this research aims to provide a comprehensive assessment of cybersecurity vulnerabilities and propose feasible solutions for the organizations, several limitations and challenges may affect the study's execution and generalizability (Creswell and Creswell, 2018).

These are outlined below:

1.8.1 Limited Access to Confidential Information: Some cybersecurity-related documents, such as detailed incident reports, network configurations, and system logs, are confidential. The organization may restrict access to these sensitive records due to security concerns. This may limit the depth of technical analysis the research can conduct.

1.8.2 Time Constraints: The study must be completed within the academic semester timeline. Cybersecurity assessments and interviews can require extended observation and data collection, but the available time limits the breadth of data that can be gathered and analyzed.

1.8.3 Participant Bias in Self-Reporting: Data collection methods such as questionnaires and interviews rely on the honesty and willingness of participants. Some employees may underreport careless cybersecurity behavior (e.g., using weak passwords, opening phishing emails) due to fear of blame, leading to biased responses.

1.8.4 Limited Cybersecurity Awareness Among Employees: Some respondents may have a limited understanding of cybersecurity concepts, which could result in incomplete or inaccurate responses. This may affect the reliability of questionnaire results.

1.8.5 Restricted Generalizability of Findings: The research focuses exclusively on the organizations, a private engineering firm in Zimbabwe. Although findings may be useful to similar organizations, results cannot be generalized to larger corporations or companies operating in different industries or regulatory environments.

1.8.6 Financial and Resource Constraints: The research does not involve live penetration testing or advanced technical audits because such activities require specialized tools, skills, and financial resources that are beyond the scope of this academic study.

1.8.7 Dependence on Organizational Cooperation: Successful data collection depends on management approval and the willingness of employees to participate. If staff availability or cooperation is limited, data collection may be delayed or incomplete.

1.9 SCOPE / DELIMITATION OF THE RESEARCH

The scope and delimitations define the boundaries of what the research will cover and intentionally exclude, ensuring the study remains focused and manageable within the available time and resources.

1.9.1 Scope of the Study

This research focuses on ten private firms in Zimbabwe where IT students undertook industrial internships. These firms operate across five sectors: engineering and construction, financial services, manufacturing, retail and distribution, and telecommunications. The study examines the cybersecurity environment across these organizations, focusing on the following areas:

1. Technical Aspects of Cybersecurity

i. Assessment of network and system security controls observed by students

ii. Protection of organizational data practices at host organizations

iii. Access control and authentication practices observed

iv. Use of software, hardware, and cloud systems across organizations

v. Vulnerability management practices (or absence thereof)

2. Human and Behavioral Aspects

i. Employee cybersecurity awareness and training levels observed at host organizations

ii. Password practices, email usage, and handling of sensitive information

iii. User behavior and how it contributes to cybersecurity vulnerabilities

iv. Management attitudes toward cybersecurity as reported by students

3. Organizational Policies and Governance

i. Review of existing cybersecurity policies and procedures at host organizations

ii. Analysis of incident response processes (where documented)

iii. Evaluation of management's role in cybersecurity enforcement

4. Comparison with Cybersecurity Frameworks

i. Understanding how international frameworks (ISO 27001 and NIST) can be applied in SME contexts

ii. Identifying gaps between current practices across organizations and recommended standards

Data was collected through questionnaires administered to the ten IT students, who provided information based on their observations, informal interviews with staff at their host organizations, and review of available documentation during their internship periods.

1.9.2 Delimitations (What the Study Will Not Cover)

To maintain focus, the research is limited by the following boundaries:

1. **Geographical Delimitation:** The study only covers private firms operating within Zimbabwe. Organizations with operations outside Zimbabwe are excluded.

2. **Participant Delimitation:** Only the ten IT students who were classmates of the researcher participated in formal data collection. While students gathered observations from staff at their host organizations, those staff members were not directly surveyed or interviewed by the researcher. Students served as the primary respondents, reporting on their observations and access to documentation.

3. **Sectoral Delimitation:** The study covers five sectors (engineering, financial services, manufacturing, retail, telecommunications). Findings may not be generalizable to other sectors such as healthcare, education, or government.

4. **Technological Scope:** The research examines current operational systems observed by students during their internship periods. Legacy systems no longer in use are not assessed. The study does not involve live penetration testing or ethical hacking due to ethical, financial, and operational constraints.

5. **Time Delimitation:** The study focuses on cybersecurity incidents and practices observed during the students' internship periods (approximately 3-6 months per student). Historical incidents before this period are only included where documented and reported by students.

6. **Financial Delimitation:** The research does not invest in or procure advanced cybersecurity tools. Analysis is based on observations reported by students, information

gathered from the host organization's documentation, and comparisons with established frameworks.

1.10 DEFINITION OF TERMS

This section provides operational definitions of key terms used in the study. Defining these terms ensures a common understanding of the concepts throughout the research (Kumar, 2019).

1. **Cybersecurity:** Refers to the practices, technologies, and processes used to protect computers, networks, systems, and data from unauthorized access, cyber-attacks, damage, or theft (Stallings and Brown, 2018).
2. **Information Security:** A broader concept that involves protecting information (whether digital or physical) from unauthorized access, disclosure, alteration, and destruction (Von Solms and Van Niekerk, 2013).
3. **Cyber-attack:** Any deliberate attempt to gain unauthorized access to a computer system or network with the intent to cause harm, steal information, or disrupt operations. Examples include phishing, malware, ransomware, and hacking (Hadnagy, 2018).
4. **Threat:** Any potential danger that could exploit a vulnerability and cause harm to an organization's information or systems (NIST, 2024).
5. **Vulnerability:** A weakness or flaw in a system (software, hardware, or human behavior) that a cyber threat or attacker can exploit (ISO, 2022).
6. **Risk:** The possibility that a cyber threat will exploit a vulnerability and negatively affect the organization — typically measured in terms of likelihood and impact (Hubbard, 2020).
7. **Data Breach:** An incident where unauthorized individuals gain access to confidential or sensitive information (Ponemon Institute, 2023).
8. **Access Control:** Security measures that ensure only authorized users can access certain systems, data, or resources (Kim and Solomon, 2020).
9. **Confidentiality:** Ensuring that information is only accessible to individuals who are authorized to view it (Stallings and Brown, 2018).
10. **Integrity:** Ensuring that information is accurate, complete, and has not been tampered with (Von Solms and Van Niekerk, 2013).

11. **Availability:** Ensuring that systems and information are accessible to authorized users whenever needed (NIST, 2024).
12. **ISO 27001:** An international standard that provides a framework for establishing, implementing, and maintaining an effective information security management system (ISMS) (ISO, 2022).
13. **NIST Framework:** A cybersecurity framework developed by the U.S. National Institute of Standards and Technology used to help organizations identify, protect, detect, respond to, and recover from cyber threats (NIST, 2024).
14. **Cyber and Data Protection Act:** Zimbabwe's legislation enacted in 2018 to provide a legal framework for cybersecurity and data protection (Government of Zimbabwe, 2018).
15. **CERT:** Computer Emergency Response Team - an organization that coordinates incident response and provides cybersecurity guidance (CERT Zimbabwe, 2024).
16. **SME (Small and Medium Enterprise):** A business entity that has a limited number of employees, asset value, and revenue compared to large corporations. For this research, the organization is classified as an SME (Moyo and Sibanda, 2021).

1.11 SUMMARY

This chapter introduced the study by outlining the background, context, and motivation for improving cybersecurity at the organizations. The problems of limited cybersecurity awareness, inadequate policies, and a lack of proactive monitoring were highlighted, emphasizing the need for a structured, cost-effective solution. The research objectives and questions were clearly defined, supporting the justification for employing a mixed-method approach to investigate vulnerabilities and develop practical interventions. The scope, limitations, and key terms were also presented, establishing a foundation for the literature review in Chapter 2

CHAPTER 2

LITERATURE REVIEW

2.1 INTRODUCTION

This chapter reviews published work on cybersecurity, with a particular focus on issues affecting engineering firms and small and medium-sized enterprises (SMEs). The aim is to show what other researchers have discovered, identify gaps in existing knowledge, and connect these findings to the current study. The review begins with theories commonly used to explain cybersecurity behavior and risk management. It then examines both theoretical and empirical studies on cybersecurity challenges, employee awareness, international frameworks, and the specific issues faced by SMEs in developing countries, with particular emphasis on Zimbabwe. According to Creswell and Creswell (2018), a comprehensive literature review enables researchers to situate their work within the existing body of knowledge and identify areas requiring further investigation.

2.2 CONCEPTUAL FRAMEWORK

The conceptual framework for this study integrates three key domains: cybersecurity vulnerabilities in SMEs, human factors in information security, and international cybersecurity standards (ISO 27001 and NIST). These concepts provide the foundation for understanding the cybersecurity challenges faced by the organizations.

2.2.1 Cybersecurity Vulnerabilities in SMEs

Research consistently demonstrates that SMEs face distinctive cybersecurity challenges. Sharma and Gupta (2022) conducted a comprehensive study of 200 SMEs across multiple sectors, finding that 68% had experienced at least one security incident in the preceding year. The research identified several contributing factors, including limited dedicated security staff, reliance on informal practices, and insufficient security budgets. Organizations with fewer than 50 employees were particularly vulnerable, often lacking any dedicated security personnel.

Alshaikh (2020) examined why SMEs struggle to implement effective security measures, conducting interviews with IT personnel at 45 organizations. The study revealed that competing business priorities consistently overshadowed security concerns. Managers focused on customer acquisition, cash flow management, and operational efficiency, viewing security as a

secondary concern until an incident occurred.

In Zimbabwe, POTRAZ (2023) reported a 35% increase in cyber incidents targeting SMEs between 2022 and 2023. Chikwanha (2023) investigated this trend through a survey of 150 SMEs in Harare and Bulawayo, identifying a lack of awareness, limited budgets, and the absence of formal policies as primary challenges. Only 12% of surveyed organizations had documented security policies, and just 8% conducted regular security awareness training.

2.2.2 Human Behavior and Cybersecurity Awareness

The relationship between human behavior and security incidents has been extensively studied. Parsons, McCormac, Butavicius and Ferguson (2019) conducted an 18-month longitudinal study tracking employees' security behaviors, finding that without regular training, phishing susceptibility remained consistently high. Employees who received quarterly training showed gradual improvement, while those who received only initial training showed no significant change in behavior over time.

Alotaibi (2021) examined password practices among SME employees, surveying 300 workers across 45 organizations. The study found that 67% of respondents admitted to reusing passwords across multiple accounts, and 43% reported sharing credentials with colleagues. These practices create significant security vulnerabilities by increasing the impact of any single credential compromise.

2.2.3 International Cybersecurity Frameworks

International frameworks provide structured approaches to cybersecurity management. ISO 27001, most recently updated in 2022, specifies requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISO, 2022). Kim and Solomon (2020) explain that ISO 27001 helps organizations create clear policies, systematically reduce risks, and manage incidents efficiently through documented procedures and regular audits.

The NIST Cybersecurity Framework offers a more flexible alternative. Version 2.0 (NIST, 2024) organizes cybersecurity activities into five functions: Identify, Protect, Detect, Respond, and Recover. Each function includes categories and subcategories that organizations can implement based on their specific risks and resources. Chen and Zhao (2021) found that SMEs can achieve significant security improvements by implementing selected components of the framework without the full resource commitment required for ISO 27001 certification.

Mutambara and Vhutshilo (2021) adapted the NIST framework specifically for Zimbabwean SMEs and tested their approach with 15 organizations over six months. Participating firms implemented basic controls from the Identify and Protect functions, including asset inventory, access control, and awareness training. The pilot program achieved a 40% reduction in security incidents, demonstrating that significant improvements are possible without expensive tools.

2.3 THEORETICAL FRAMEWORK

2.3.1 Information Security Theory

Information Security Theory provides the foundation for understanding how organizations protect their digital assets. Stallings and Brown (2018) explain that this theory centers on three core principles: confidentiality, integrity, and availability, commonly known as the CIA triad. Confidentiality ensures that information is accessible only to authorized individuals, integrity guarantees that data remains unaltered during storage or transmission, and availability ensures that information is accessible when needed. Von Solms and Van Niekerk (2013) extend this framework by arguing that effective information security requires more than technical solutions; it demands a combination of technological tools, organizational policies, and employee awareness. Kim and Solomon (2020) support this view, noting that security failures often result from weaknesses in people and processes rather than technology alone.

For engineering firms, these theoretical principles have particular significance. Peterson and Lee (2022) observe that engineering organizations store sensitive intellectual property, including design documents, client specifications, and proprietary methodologies. When confidentiality is compromised, firms may lose a competitive advantage. When integrity is violated, engineering calculations or design specifications could be altered, potentially leading to structural failures or safety incidents. However, Moyo and Sibanda (2021) note that implementing the CIA triad proves challenging for SMEs with limited resources. The tension between security and operational efficiency often results in compromises that leave organizations vulnerable.

2.3.2 Risk Management Theory

Risk Management Theory offers a structured approach to security decision-making. Hubbard (2020) defines risk management as the systematic process of identifying, analyzing, and

responding to risks across an organization's operations. The theory posits that organizations cannot eliminate all threats but can prioritize responses based on likelihood and potential impact. ISO (2018) codifies this approach in the ISO 31000 Risk Management Standard, which provides principles and guidelines for managing risks across any organization.

NIST (2024) incorporates risk management as a central component of its cybersecurity framework, emphasizing that organizations should focus resources on the most significant threats rather than attempting to address every possible vulnerability. This risk-based approach proves particularly valuable for SMEs, which typically lack the resources of larger enterprises. Chen and Zhao (2021) found that SMEs adopting risk-based approaches achieved better security outcomes with limited budgets by focusing on controls that addressed their most probable threats. Furnell and Clarke (2020) argue that many SMEs waste limited resources on security measures that fail to address their actual risks, highlighting the importance of conducting a proper risk assessment before selecting controls.

2.3.3 Human Factors Theory

Human Factors Theory examines the role of human behavior in security incidents. Reason (1990), in foundational work on human error, distinguished between active failures (immediate actions with immediate consequences) and latent conditions (underlying organizational factors that create error-prone environments). Parsons, McCormac, Butavicius, and Ferguson (2019) apply these concepts to cybersecurity, finding that employee behavior accounts for a substantial proportion of security incidents in organizations. Their research demonstrates that even sophisticated technical controls can be circumvented by well-intentioned employees who lack awareness of security risks.

Hadnagy (2018) explores how attackers exploit human psychology through social engineering techniques. The author documents methods by which attackers manipulate trust, create false urgency, and exploit natural human helpfulness to gain unauthorized access. Alotaibi (2021) quantified the impact of human factors in SMEs, finding that approximately 80% of security incidents involved some element of human error or manipulation. These findings underscore the importance of employee awareness as a critical component of any cybersecurity strategy, particularly in organizations where technical controls may be limited.

These three theories were selected because they collectively address the core dimensions of cybersecurity in SMEs: Information Security Theory provides the technical foundation (confidentiality, integrity, availability), Risk Management Theory enables prioritization of

security investments under resource constraints, and Human Factors Theory accounts for employee behavior, which is the weakest link in most organizational security postures.

2.4 EMPIRICAL EVIDENCE

2.4.1 Cybersecurity Challenges in SMEs

Research consistently demonstrates that SMEs face distinctive cybersecurity challenges. Sharma and Gupta (2022) conducted a comprehensive study of 200 SMEs across multiple sectors, finding that 68% had experienced at least one security incident in the preceding year. The research identified several contributing factors, including limited dedicated security staff, reliance on informal practices, and insufficient security budgets. Organizations with fewer than 50 employees were particularly vulnerable, often lacking any dedicated security personnel.

Alshaikh (2020) examined why SMEs struggle to implement effective security measures by interviewing IT personnel at 45 organizations. The study revealed that competing business priorities consistently overshadowed security concerns. Managers focused on customer acquisition, cash flow management, and operational efficiency, viewing security as a secondary concern until an incident occurred. This reactive approach to security, while understandable given resource constraints, left organizations exposed to threats that could have been prevented with proactive measures.

The scale of the threat to SMEs is documented in the Verizon Data Breach Investigations Report (Verizon, 2024), which found that 43% of cyber-attacks target small businesses. Despite this disproportionate targeting, only 14% of SMEs consider themselves adequately prepared to defend against attacks. Furnell and Clarke (2020) describe this situation as a "cybersecurity gap": SMEs are too large to rely on simple security practices suitable for micro-enterprises but too small to afford the dedicated security teams and sophisticated tools used by large corporations.

In Zimbabwe, POTRAZ (2023) reported a 35% increase in cyber incidents targeting SMEs between 2022 and 2023. Chikwanha (2023) investigated this trend through a survey of 150 SMEs in Harare and Bulawayo, identifying a lack of awareness, limited budgets, and the absence of formal policies as primary challenges. Only 12% of surveyed organizations had documented security policies, and just 8% conducted regular security awareness training. CERT Zimbabwe (2024) noted that under-reporting of incidents complicates efforts to understand the full scope of the problem, as many SMEs do not report incidents due to concerns about reputational damage.

2.4.2 Cybersecurity Vulnerabilities in Engineering Firms

Engineering firms present unique security challenges due to the nature of their work and the systems they employ. Wang, Chen, and Zhang (2021) studied 85 engineering firms and found that 73% were running operating systems that vendors no longer supported. This reliance on legacy software creates unpatched vulnerabilities that attackers can exploit. The researchers noted that engineering organizations often prioritize system stability and compatibility over security updates, particularly when specialized engineering software requires specific operating system versions.

Peterson and Lee (2022) examined intellectual property theft in engineering firms, documenting several cases in which competitor nations sponsored attacks targeting engineering designs and specifications. The study found that engineering drawings, manufacturing specifications, and proprietary methodologies were prime targets for industrial espionage. Once compromised, such intellectual property cannot be recovered, and the competitive advantage it represents may be permanently lost.

The convergence of information technology and operational technology creates additional vulnerabilities in engineering environments. Stouffer, Falco, and Scarfone (2023) from NIST explain that while IT/OT convergence improves efficiency by enabling data sharing between business and production systems, it also exposes previously isolated control systems to internet-based threats. Unlike IT systems, OT systems often run on proprietary protocols, have long lifecycles measured in decades rather than years, and cannot be easily patched without disrupting physical processes. These characteristics create complex security challenges that require specialized approaches.

In Zimbabwe, Mandizha and Chirume (2021) assessed security practices at engineering firms in Harare and found that most lacked basic controls, such as network segmentation and access control lists. Engineering drawings and project documentation were frequently stored on unprotected file servers or shared via unsecured cloud platforms. The study revealed that 82% of surveyed firms had experienced intellectual property theft, though only 23% could definitively attribute losses to cyber incidents. This uncertainty about the source of intellectual property losses complicates efforts to justify security investments.

2.4.3 Human Behavior and Cybersecurity Awareness

The relationship between human behavior and security incidents has been extensively studied. Parsons, McCormac, Butavicius, and Ferguson (2019) conducted an 18-month longitudinal

study tracking employee security behaviors, finding that without regular training, phishing susceptibility remained consistently high. Employees who received quarterly training showed gradual improvement, while those who received only initial training showed no significant change in behavior over time. This finding suggests that one-time awareness campaigns are insufficient to change behavior.

Alotaibi (2021) examined password practices among SME employees, surveying 300 workers across 45 organizations. The study found that 67% of respondents admitted to reusing passwords across multiple accounts, and 43% reported sharing credentials with colleagues. These practices, while convenient for employees, create significant security vulnerabilities by increasing the impact of any single credential compromise. The research also found that employees who understood the risks associated with poor password practices were significantly less likely to engage in risky behaviors.

Hadnagy (2018) provides a detailed analysis of social engineering techniques, demonstrating how attackers exploit psychological principles to bypass technical controls. The author documents methods including pretexting (creating fictional scenarios to obtain information), phishing (using fraudulent emails to solicit information), and baiting (offering something enticing to deliver malware). These techniques succeed not because technical controls fail, but because human psychology is predictable and can be manipulated.

The effectiveness of phishing attacks correlates strongly with employee awareness levels. Chikwanha (2023) found that in Zimbabwean SMEs, only 28% of employees could identify common phishing indicators such as suspicious sender addresses, urgent requests, or grammatical errors. Only 15% knew the correct procedure for reporting suspicious emails. POTRAZ (2023) has attempted to address this through a national awareness campaign incorporating workshops, radio programs, and online resources. However, Mutambara and Vhutshilo (2021) argue that continuous, role-based training proves more effective than one-time campaigns, as knowledge retention decays rapidly without reinforcement.

2.4.4 International Cybersecurity Frameworks (ISO 27001 and NIST)

International frameworks provide structured approaches to cybersecurity management. ISO 27001, most recently updated in 2022, specifies requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISO, 2022). The standard covers organizational context, leadership commitment, planning, support, operation, performance evaluation, and improvement. Kim and Solomon (2020) explain that

ISO 27001 helps organizations create clear policies, systematically reduce risks, and manage incidents efficiently through documented procedures and regular audits.

However, implementation challenges limit the adoption of ISO 27001 among SMEs. Moyo and Sibanda (2021) note that the resource requirements for certification, including documented procedures, regular audits, and continuous improvement processes, exceed the capacity of many small organizations. The cost of external auditors and the time required for internal documentation create barriers that discourage SME participation.

The NIST Cybersecurity Framework offers a more flexible alternative. Version 2.0 (NIST, 2024) organizes cybersecurity activities into five functions: Identify, Protect, Detect, Respond, and Recover. Each function includes categories and subcategories that organizations can implement based on their specific risks and resources. Chen and Zhao (2021) found that SMEs can achieve significant security improvements by implementing selected components of the framework without the full resource commitment required for ISO 27001 certification. Their research developed a prioritized implementation guide that focuses on the most critical controls based on threat frequency and impact.

Mutambara and Vhutshilo (2021) adapted the NIST framework specifically for Zimbabwean SMEs and tested their approach with 15 organizations over six months. Participating firms implemented basic controls from the Identify and Protect functions, including asset inventory, access control, and awareness training. The pilot program achieved a 40% reduction in security incidents, demonstrating that significant improvements are possible without expensive tools or extensive consulting support. This finding has important implications for organizations operating with limited resources.

2.4.5 Cloud Security in Engineering SMEs

Cloud computing adoption continues to grow among engineering SMEs due to benefits including reduced infrastructure costs, improved collaboration, and access to advanced tools. Hashizume, Rosado, Fernández-Medina, and Fernández (2020) analyzed cloud security incidents and identified common vulnerabilities, including misconfigured storage, inadequate access controls, and insufficient data encryption. Their research found that many cloud breaches resulted not from sophisticated attacks but from simple configuration errors that exposed data to public access.

The Cloud Security Alliance (CSA, 2023) provides guidance specifically for SMEs adopting cloud services, emphasizing the shared responsibility model, in which cloud providers secure the infrastructure while customers secure their data and access. Many SMEs misunderstand this division, if cloud providers assume full security responsibility. Peterson and Lee (2022) recommend that engineering firms implement encryption for sensitive data, enforce strong access controls, and conduct regular cloud security audits to verify configurations.

In Zimbabwe, cloud adoption among SMEs is increasing, but security practices lag. Moyo and Sibanda (2021) found that while 67% of surveyed SMEs used some cloud services, only 23% had implemented basic security measures such as multi-factor authentication or data encryption. Mandizha and Chirume (2021) noted that many engineering firms use consumer-grade cloud services without understanding the security implications, exposing sensitive project data to unnecessary risk. Engineering drawings and client specifications stored in unsecured cloud environments represent significant intellectual property vulnerabilities.

2.4.6 Financial Impact of Cyber-attacks

The financial consequences of cyber-attacks on SMEs are substantial and often underestimated. The Ponemon Institute (2023) reported that the average cost of a data breach for SMEs reached $3.31 million, a 15% increase from the previous year. These costs include direct expenses such as incident response, legal fees, and regulatory fines, as well as indirect costs including business disruption, customer churn, and reputational damage.

Accenture (2022) found that 60% of SMEs that suffer a significant cyber-attack go out of business within six months. This striking statistic highlights the existential threat that cyber incidents pose to small businesses with limited financial reserves. Even organizations that survive attacks may face prolonged recovery periods during which normal operations are disrupted, and customer confidence erodes.

In Zimbabwe, CERT Zimbabwe (2024) documented several cases where SMEs incurred significant financial losses due to ransomware attacks. One engineering firm reportedly lost ZWL$5 million in project delays and recovery costs following a ransomware incident that encrypted critical design files. The organization lacked adequate backups and was forced to either pay the ransom or reconstruct months of work. This case illustrates how technical vulnerabilities translate directly into financial harm when organizations lack proper preparation.

2.4.7 Cybersecurity Policies and Governance

Documented cybersecurity policies play a crucial role in establishing security expectations and accountabilities. Karanja (2020) studied organizations with and without formal security policies, finding that those without documented policies were significantly more likely to experience repeated security problems. Policies guide acceptable behavior, incident-handling procedures, and access-control requirements, creating consistent expectations across the organization.

Doherty, Anastasakis, and Fulford (2021) emphasize that simply having policy documents is insufficient; policies must be communicated effectively and enforced consistently. Their research found that organizations with strong policy communication and enforcement mechanisms achieved better security outcomes than those with comprehensive but unenforced policies. Employees must understand their responsibilities and the consequences of non-compliance with policies to influence behavior.

NIST (2024) recommends regular policy reviews and updates to reflect changing threats and business requirements. Static policies quickly become outdated as technology evolves, and new threats emerge. Organizations should establish review cycles that ensure policies remain relevant and continue to address current risks.

In Zimbabwe, the Cyber and Data Protection Act (Government of Zimbabwe, 2018) requires organizations to implement data protection policies and report breaches. However, Mandizha and Chirume (2021) found that compliance remains low among SMEs due to a lack of awareness and limited resources. POTRAZ (2023) is working with industry associations to develop template policies that SMEs can adapt, recognizing that many organizations lack the expertise to develop comprehensive policies independently.

2.4.8 Low-Cost Cybersecurity Measures

Research demonstrates that effective cybersecurity does not necessarily require expensive tools. Mutambara and Vhutshilo (2021) showed that SMEs can strengthen security through affordable measures, including multi-factor authentication, properly configured firewalls, up-to-date antivirus software, and strong password policies. Their study of Zimbabwean SMEs found that organizations implementing these basic controls experienced significantly fewer security incidents than those relying on minimal protection.

The Center for Internet Security (CIS, 2023) publishes a set of critical security controls prioritized for SMEs. These controls include inventorying authorized devices, securely configuring hardware and software, continuously managing vulnerabilities, and controlling the use of administrative privileges. Implementing these controls can prevent approximately 85% of common attacks, according to CIS analysis of incident data.

Chen and Zhao (2021) found that open-source security tools can provide enterprise-grade protection at no cost. Tools such as pfSense for firewall functionality, ClamAV for antivirus protection, and Wazuh for security monitoring offer viable alternatives to commercial products. This finding is relevant to Zimbabwean SMEs facing foreign-currency constraints that make commercial software licenses prohibitively expensive. Organizations can achieve significant security improvements by leveraging freely available tools combined with proper configuration and maintenance.

2.4.9 Cybersecurity in Developing Countries

Developing countries face distinctive cybersecurity challenges that differ from those in developed economies. Moyo and Sibanda (2021) examined the Zimbabwean context, identifying weak ICT budgets, limited infrastructure, and shortages of cybersecurity professionals as major barriers to effective security. These challenges compound the difficulties that SMEs everywhere face, creating environments where organizations are particularly vulnerable to attacks.

The International Telecommunication Union (ITU, 2023) ranks Zimbabwe 112th out of 194 countries in its Global Cybersecurity Index, indicating significant room for improvement. The index measures commitment to cybersecurity across five pillars: legal measures, technical measures, organizational measures, capacity development, and cooperation. While Zimbabwe has made progress with the Cyber and Data Protection Act (Government of Zimbabwe, 2018) and the establishment of CERT Zimbabwe (2024), implementation gaps remain significant.

Chikwanha (2023) notes that developing countries face unique challenges, including limited internet penetration, high costs of security tools due to currency constraints, and brain drain of cybersecurity professionals to developed countries that offer higher salaries. These factors combine to create environments where SMEs are particularly vulnerable to cyber threats. Organizations must develop approaches that work within local constraints rather than simply importing solutions designed for different contexts.

2.4.10 Incident Response and Recovery

Effective incident response can significantly reduce the impact of security incidents. Woods and Simpson (2022) studied organizations with documented incident response plans and found that they recovered more quickly and experienced fewer repeat incidents than organizations without such plans. Their research demonstrates that preparation, not just prevention, is essential for minimizing harm when incidents occur.

Cichonski, Millar, Grance, and Scarfone (2022) from NIST provide a detailed incident-handling guide covering preparation, detection, analysis, containment, eradication, and recovery. The guide emphasizes that organizations should practice incident response through regular exercises to ensure readiness when real incidents occur. Testing reveals gaps in plans and procedures that can be addressed before they matter.

NIST (2024) includes Respond and Recover as core functions of its cybersecurity framework, recognizing that even well-defended organizations will eventually experience security incidents. The ability to respond effectively and recover quickly distinguishes organizations that survive incidents from those that suffer prolonged disruption.

In Zimbabwe, CERT Zimbabwe (2024) provides incident response services and guidance to organizations. However, Chikwanha (2023) found that most SMEs are unaware of these services or do not know how to access them. The study recommends that SMEs develop simple incident response plans tailored to their resources and capabilities, recognizing that complex plans requiring specialized expertise may be unrealistic for smaller organizations.

2.4.11 Cybersecurity Legislation in Zimbabwe

The Cyber and Data Protection Act [Chapter 12:07] (Government of Zimbabwe, 2018) establishes the legal framework for cybersecurity in Zimbabwe. The Act establishes the Cyber Security Center, defines cyber offenses, including unauthorized access, data interception, and system interference, and sets out requirements for data protection. Organizations must register with the Cyber Security Center as data controllers, implement appropriate security measures, and notify affected individuals in the event of a breach.

Mandizha and Chirume (2021) provide a detailed analysis of the Act, noting that while it provides a solid legal foundation, implementation and enforcement remain challenging. The Act's provisions are comprehensive, but awareness among affected organizations is limited.

Non-compliance can result in fines of up to Level 14 or imprisonment, but few organizations understand their obligations well enough to achieve compliance.

POTRAZ (2023) has developed regulations and guidelines to support implementation of the Act, including data protection guidelines for businesses and consumer education materials. CERT Zimbabwe (2024) complements these efforts by providing technical guidance and incident response coordination. However, Moyo and Sibanda (2021) found that awareness of these resources among SMEs remains low, suggesting the need for more proactive outreach.

2.5 RESEARCH GAP ANALYSIS

The literature reviewed in this chapter reveals several gaps that this study addresses:

Limited Focus on Engineering SMEs in Zimbabwe: Most research focuses on SMEs in developed countries or generic SME populations. Few studies have specifically examined engineering firms in Zimbabwe, which face unique challenges, including handling sensitive intellectual property, reliance on specialized software, and limited ICT budgets (Moyo and Sibanda, 2021).

Lack of Integrated Solutions: Existing research tends to address awareness, policies, and incident response as separate issues. There is limited evidence of integrated solutions that combine training, policy management, and incident reporting in a single, cost-effective platform suitable for SMEs (Mutambara and Vhutshilo, 2021).

Limited Empirical Testing of Low-Cost Solutions: While researchers advocate for low-cost cybersecurity measures, few studies provide empirical evidence of their effectiveness in real SME environments, particularly in developing countries (Chen and Zhao, 2021).

Insufficient Attention to Phishing Awareness: Despite phishing being the most common attack vector for SMEs (Verizon, 2024), there is limited research on effective, low-cost phishing simulation tools tailored for SMEs in developing contexts (Chikwanha, 2023).

Implementation Gaps in Cybersecurity Legislation: Research indicates a significant gap between Zimbabwe's cybersecurity legislation and actual implementation in SMEs (Mandizha and Chirume, 2021). There is a need for practical tools that help SMEs achieve compliance without extensive resources.

This study addresses these gaps by developing and testing the Integrated Cybersecurity Management System (ICMS), a cost-effective solution incorporating training,

policy management, incident reporting, and phishing simulation modules, specifically designed for an engineering SME in Zimbabwe.

2.6 SUMMARY

This chapter reviewed the literature on cybersecurity vulnerabilities in SMEs, with particular focus on engineering firms and the Zimbabwean context. The conceptual framework integrated three key domains: cybersecurity vulnerabilities, human factors, and international frameworks. The theoretical framework drew on Information Security Theory, Risk Management Theory, and Human Factors Theory. Empirical evidence demonstrated that SMEs face significant cybersecurity challenges, including limited resources, lack of awareness, and absence of formal policies. International frameworks such as ISO 27001 and NIST offer structured approaches but require adaptation for resource-constrained environments. The research gap analysis identified five key gaps addressed by this study. Overall, the literature indicates that private firms in Zimbabwe need a structured and affordable cybersecurity strategy addressing both technical controls and human-centred interventions.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 INTRODUCTION

This chapter explains the methods and procedures used to collect, analyze, and interpret the study data. It outlines the research design, population and sample, research instruments, reliability and validity measures, data collection procedures, and ethical considerations. According to Saunders, Lewis, and Thornhill (2019), the research methodology provides the blueprint for how a study is conducted, ensuring that the findings are valid, reliable, and capable of answering the research questions. This chapter also presents the system design and development process for the Integrated Cybersecurity Management System (ICMS), including hardware and software requirements, system architecture, development tools, and implementation phases.

3.2 RESEARCH DESIGN

This study adopted a mixed-methods research design that combines quantitative and qualitative approaches. The use of mixed methods was appropriate for this study because cybersecurity involves both measurable aspects (such as frequency of incidents, awareness levels, and system vulnerabilities) and subjective aspects (such as employee perceptions, attitudes, and experiences). According to Creswell and Creswell (2018), mixed methods research provides a more complete understanding of research problems than either quantitative or qualitative approaches alone.

3.2.1 Quantitative Approach

A quantitative approach was used to collect data on employees' cybersecurity awareness, password habits, exposure to threats, and incident frequency. This was mainly achieved through structured questionnaires. Kothari (2019) explains that quantitative research is useful for collecting numerical data that can be analyzed statistically to identify patterns and relationships. In this study, quantitative data helped establish baseline metrics for cybersecurity awareness levels and vulnerability frequencies across the organizations.

3.2.2 Qualitative Approach

A qualitative approach was used to obtain in-depth information from management and IT personnel regarding internal policies, challenges, existing controls, and their perceptions of cybersecurity readiness. This was done through interviews and document analysis. Kumar (2019) notes that qualitative research is valuable for exploring complex phenomena and understanding the context in which decisions are made. The qualitative component of this study provided rich insights into the organizational culture, management attitudes, and practical challenges that quantitative data alone could not capture.

3.2.3 Justification for Mixed Methods

The mixed-method design was chosen for several reasons. First, cybersecurity is a multidimensional issue involving technology, people, and processes (Von Solms and Van Niekerk, 2013). A single method cannot adequately capture all these dimensions. Second, triangulation of findings from different sources enhances the validity and reliability of conclusions (Saunders, Lewis, and Thornhill, 2019). Third, the research questions required both numerical data (e.g., "how many incidents?") and explanatory data (e.g., "why do incidents occur?"). The mixed-method design accommodates both types of questions effectively.

3.3 POPULATION AND SAMPLE

3.3.1 Target Population

The target population for this study consisted of Information Technology students from the researcher's academic program who were on industrial internship at various private firms in Zimbabwe during the 2023-2024 academic period. According to program records, approximately 45 students from the Network Engineering program were placed at different organizations across Zimbabwe during this period. These students were eligible to participate because their internship placements provided them with direct exposure to ICT environments, cybersecurity practices, and operational challenges within private-sector organizations.

Kumar (2019) defines the target population as the complete set of individuals or elements that possess the information sought by the researcher and about which inferences are to be made. In this study, IT students on internship were selected because they occupy a unique position—they are neither permanent employees nor external consultants, allowing them to observe organizational practices objectively while having access to ICT systems and documentation as part of their internship duties.

3.3.2 Sample Size

A sample of ten (10) IT students was selected to participate in the study. The sample was drawn from the researcher's classmates who were on an internship during the research period. This sample size was chosen for several reasons:

First, the sample ensures representation across different industry sectors. The ten students were attached to organizations across five sectors: engineering and construction (3 students), financial services (2 students), manufacturing (2 students), retail and distribution (2 students), and telecommunications (1 student). This diversity enables cross-sectoral comparisons of cybersecurity practices and challenges.

Second, a sample size of 10 is appropriate for qualitative and mixed-methods research, where the focus is on depth of information rather than statistical generalizability. Saunders, Lewis, and Thornhill (2019) note that in qualitative research, sample size is less important than the richness of data obtained. The emphasis is on selecting participants who can provide meaningful insights based on their direct observations and experiences.

Third, the sample represents approximately 22% of the eligible population of IT students on internship, which is acceptable for a case study approach involving multiple cases (ten organizations represented through student respondents).

3.3.3 Sampling Techniques

Purposive sampling was used to select the ten participating students. This sampling method was appropriate because:

i. Students were required to be on an active industrial internship during the research period
ii. Students needed to have access to ICT systems and documentation at their host organizations
iii. Students needed to represent a variety of industry sectors to enable comparative analysis
iv. Students needed to be willing to participate and provide honest observations

Patton (2015) explains that purposive sampling involves selecting information-rich cases that can provide deep insights into the research problem. The ten selected students were chosen because their internship placements offered varied organizational contexts, providing a

comprehensive view of cybersecurity challenges across Zimbabwe's private sector.

3.4 RESEARCH INSTRUMENTS

Different instruments were used to collect data from the participating IT students. These instruments were developed based on the research objectives, literature review, and established measurement tools from previous studies. The research supervisor reviewed each instrument and pilot-tested it with two IT students (who were on internship but not part of the final sample) to identify ambiguities and improve clarity.

3.4.1 Questionnaires

The questionnaire consisted of closed and open-ended questions aimed at gathering information from IT students regarding:

i. Demographic information of the student and their host organization

ii. Cybersecurity awareness levels observed at the host organization

iii. Password practices and authentication methods observed

iv. ICT usage patterns observed among employees

v. Experiences with cyber threats during the internship period

vi. Understanding of company cybersecurity policies (if any existed)

vii. General attitudes towards cybersecurity observed among staff

Questionnaires were chosen because they are cost-effective, can reach respondents across different locations, and allow for consistent data collection (Saunders, Lewis, and Thornhill, 2019). The questionnaire was administered electronically to accommodate students who were at different internship locations across Zimbabwe.

The questionnaire used a combination of Likert scales (1 = Strongly Disagree to 5 = Strongly Agree), multiple-choice questions, and yes/no questions. Open-ended questions allowed students to provide detailed observations and elaborate on specific incidents or practices they witnessed.

3.4.2 Interview Guides

Semi-structured interview guides were used to collect qualitative data from the ten IT students. The guides included open-ended questions designed to gather detailed information on:

i. Specific cybersecurity incidents observed during internship

ii. Technical vulnerabilities identified in host organization systems

iii. Existing cybersecurity controls observed

iv. Policy implementation challenges observed

v. Incident response practices (or absence thereof)

vi. Resource constraints observed at host organizations

vii. Recommendations based on students' observations

The semi-structured format allowed the researcher to ask follow-up questions, probe for deeper explanations, and explore emerging themes not covered in the guide (Creswell and Creswell, 2018). Interviews were conducted virtually using video conferencing platforms, as students were located at internship sites across Zimbabwe. Each interview lasted between 30 and 45 minutes. All interviews were audio-recorded with participant consent and transcribed verbatim for analysis.

3.4.3 Document Review Checklists

A document review checklist was developed to guide students in reviewing relevant documentation available at their host organizations. The checklist included items such as:

i. Existence and currency of ICT policies

ii. Documentation of previous incidents (where accessible)

iii. Evidence of policy enforcement

iv. Access control documentation

v. Network security configurations (where available)

vi. Audit trail records

vii. Training records

Students were asked to complete this checklist based on documentation they could access during their internship. Where documents were incomplete or unavailable, this was noted as a finding, indicating weaknesses in organizational record-keeping and policy implementation. The checklist ensured consistent review across the ten organizations and helped identify gaps and inconsistencies in documentation practices (Yin, 2018).

3.5 RELIABILITY AND VALIDITY

Ensuring validity and reliability was a key consideration in the research design. Validity refers to the extent to which the research accurately measures what it intends to measure, while reliability refers to the consistency of the measurements (Kothari, 2019).

3.5.1 Validity

Content validity was ensured by basing questionnaire and interview questions on established instruments from the literature and having them reviewed by the research supervisor. Construct validity was enhanced by using multiple data sources (triangulation) to confirm findings. Internal validity was addressed by carefully analyzing relationships between variables and considering alternative explanations for observed patterns (Saunders, Lewis, and Thornhill, 2019).

3.5.2 Reliability

Reliability was enhanced through several measures. The questionnaire was pilot tested with two employees to identify ambiguous questions and ensure consistency in interpretation. Interview protocols were standardized to ensure all participants were asked similar core questions. Document analysis followed a structured checklist to ensure consistent review across documents (Yin, 2018).

3.6 DATA COLLECTION PROCESS

Data collection followed a structured process:

Phase 1: Preparatory Phase. I obtained ethical clearance from the university. I secured permission from the organization's management

i. Developed and pilot-tested research instruments

ii. Made revisions based on pilot feedback

Phase 2: Questionnaire Administration. I distributed questionnaires to 6 employees

i. Provided clear instructions and assured anonymity

ii. Collected completed questionnaires after one week

iii. Followed up with non-respondents

Phase 3: Interviews. I scheduled interviews with 4 key informants

i. Conducted interviews in private settings

ii. Audio-recorded with participant consent

iii. Transcribed interviews immediately after each session

Phase 4: Document Analysis. I requested access to the relevant documents. I reviewed documents using a checklist

i. Recorded observations and findings

ii. Cross-referenced with questionnaire and interview data

3.7 ETHICAL CONSIDERATIONS

3.7.1 Informed Consent

All participants were provided with clear information about the purpose of the study, the nature of their participation, and how their data would be used. Written informed consent was obtained before any data collection commenced. Participants were informed that their participation was voluntary and that they could withdraw at any time without penalty (Saunders, Lewis, and Thornhill, 2019).

3.7.2 Confidentiality and Anonymity

Participants were assured that their responses would be treated with strict confidentiality. Questionnaire responses were collected anonymously, with no identifying information recorded. Interview participants were assigned pseudonyms in transcripts and reports to protect their identities. All data was stored securely on password-protected devices accessible only to the researcher (Creswell and Creswell, 2018).

3.7.3 Organizational Permission

Written permission was obtained from the management of the organizations before commencing the study. The organization was assured that the research findings would be shared with them and that recommendations would be provided to improve their cybersecurity posture (Yin, 2018).

3.7.4 Data Protection

All data was handled in accordance with Zimbabwe's Cyber and Data Protection Act (Government of Zimbabwe, 2018) and general data protection principles. Personal data was minimized, anonymized where possible, and securely stored. Data will be retained only for as long as necessary for the research purposes and will be securely destroyed thereafter.

3.7.5 Organizational Anonymity

At the request of the participating organization, the organization's name and any identifying details have been withheld from this dissertation. Throughout this document, the organization is referred to as "the organization" to protect its identity. This measure was taken to encourage openness from participants and to respect the organization's concern about reputational risks associated with disclosing cybersecurity vulnerabilities.

3.8 SYSTEM DOCUMENTATION

3.8.1 Hardware Requirements

For the development and operation of the Integrated Cybersecurity Management System (ICMS), the hardware must be capable of handling the application efficiently. The essential hardware requirements include:

COMPONENT	SPECIFICATION	PURPOSE
Server/Workstation	4GB RAM minimum, 2.5GHz dual-core processor	Hosting the Flask application and database
Client Devices	Any device with a web browser (desktop, laptop, tablet)	User access to the system
Network Connection	Internet connection (1Mbps minimum)	Remote access and multi-user concurrent access
Storage	10GB available disk space	Database storage and application files
Backup Storage	External drive or cloud storage	Regular database backups

Table1: Hardware Requirements

These components are crucial to achieve the computational efficiency required for the cybersecurity management system.

3.8.2 Software Requirements

The software environment is equally important for supporting the hardware's functionality and the system's needs. The software requirements include:

SOFTWARE	**VERSION**	**PURPOSE**
Operating System	Windows 10/11, Linux (Ubuntu 20.04+), or macOS	A platform for running the application
Python	3.11 or higher	Core programming language
Flask	2.3.2	Web framework for routing and rendering
Flask- SQL Alchemy	3.0.5	ORM for database interactions
Flask-Login	0.6.2	User session management
Flask-Bcrypt	1.0.1	Password hashing and encryption

SOFTWARE	VERSION	PURPOSE
SQLite	3.x	Embedded database (included with Python)
Web Browser	Chrome, Firefox, Edge, or Safari	Client-side access
Git	Latest	Version control (development only)
VS Code	Latest	Code editor (development only)

Table 2: Software Requirements

Together, these software components create an environment conducive to the effective development and operation of the cybersecurity management system.

3.9 SYSTEM DEVELOPMENT

System development is a multi-faceted process that involves the strategic use of various tools and methodologies to build and refine the proposed ICMS. This phase is critical as it translates theoretical models and algorithms into a functional system that can be tested and evaluated.

3.9.1 System Development Tools

The development of the ICMS leverages a suite of software tools that are integral to the project's success:

Tool	Purpose	Usage in Project
VS Code	Integrated Development Environment	Writing and editing all Python and HTML code
Git	Version control	Tracking code changes, creating backup points

Tool	Purpose	Usage in Project
GitHub	Code repository	Storing code remotely (optional)
Chrome DevTools	Frontend debugging	Testing HTML/CSS rendering
SQLite Browser	Database management	Viewing and editing database tables
Postman	API testing	Testing routes during development
Pip	Package manager	Installing Python dependencies

Table 3: System Development Tools

These tools were selected for their reliability, community support, and alignment with the project's technical requirements.

3.9.2 Rapid Prototyping

The system development adopted a rapid prototyping approach, characterized by iterative cycles of prototyping, testing, and refinement. This methodology allows for:

i. **Quick Feedback:** Stakeholders can review prototypes early in the development process, providing valuable input that shapes the system's evolution.

ii. **Flexibility:** The ability to rapidly adapt to changes in requirements or objectives, ensuring the system remains aligned with the project's goals.

iii. **Risk Reduction:** Early detection and resolution of issues, minimizing the risk of costly changes later in the development cycle.

iv. **User-Centric Design:** Continuous engagement with end-users ensures that the system is tailored to their needs and preferences.

3.9.3 Feasibility Study

Technical Feasibility: The system is technically feasible because it relies on widely available, open-source technologies such as Python, Flask, and SQLite. The existing computer

infrastructure at the organizations can support the system without major hardware upgrades. The modular architecture allows for gradual implementation and testing.

Economic Feasibility: Economic feasibility is achieved using open-source software, which eliminates licensing costs. The system enhances existing infrastructure rather than requiring expensive replacements. With zero software costs and minimal hardware requirements, the system is affordable for an SME with a limited ICT budget.

Operational Feasibility: The system's user-friendly interface and automation capabilities support operational feasibility. The training modules are self-paced, policies can be acknowledged electronically, and incident reporting is streamlined. Basic training is sufficient for administrators to monitor system outputs, making adoption practical within the existing skills base.

3.10 SYSTEM ANALYSIS

System analysis is the process of studying the proposed system to understand what the system should do, how it will work, and what requirements must be met.

PRESENTATION LAYER (HTML Templates- User interface) Base.html, dashboard/
APPLICATION LAYER (Flask Routes- Business Logic) App.py- Routes
MODEL LAYER (Database Models- Data Structure) User, TrainingModule, Policy, Incident, PhishingCampain
DATA LAYER (SQLite Database- Data Storage) Icms.db

Table 4: System Analysis

3.10.1 Technical Requirements Analysis

FUNCTIONAL REQUIREMENTS:

User Authentication: Secure login and registration with role-based access control

Training Module: Interactive cybersecurity courses with quizzes and progress tracking

Policy Management: Policy repository with acknowledgment tracking

Incident Reporting: Incident creation, status tracking, and comment functionality

Phishing Simulation: Campaign management and results tracking

Dashboard: Role-specific dashboards with relevant statistics

NON-FUNCTIONAL REQUIREMENTS:

Performance: System should respond within 3 seconds

Reliability: 99% uptime during working hours

Security: Password encryption, session management, SQL injection prevention

Usability: User-friendly interface with clear navigation

Scalability: Support for up to 100 concurrent users

3.11 SYSTEM DESIGN

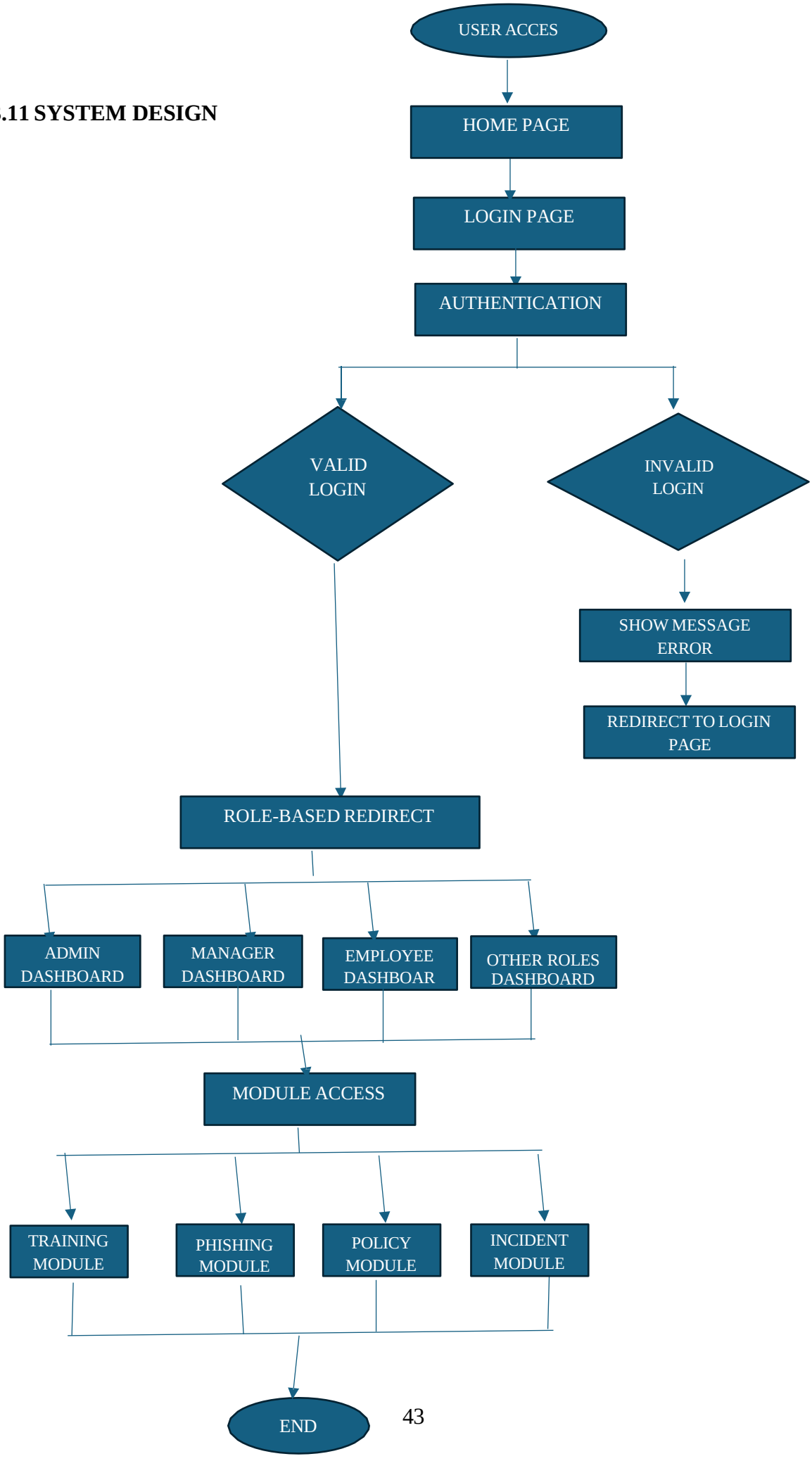


Figure 1: System Design

3.12 CODING

The system was implemented using Python Flask. Below is a key code snippet showing the incident reporting route:

```
@app.route('/incidents')
@login_required
def incidents():
    if current_user.role == 'admin':
        all_incidents = Incident.query.order_by(Incident.reported_date.desc()).all()
    elif current_user.role == 'manager':
        all_incidents = Incident.query.order_by(Incident.reported_date.desc()).all()
    else:
        all_incidents = Incident.query.filter_by(reported_by=current_user.id).order_by(Incident.reported_date.d

    return render_template('incidents/incidents.html', incidents=all_incidents)

@app.route('/incidents/new', methods=['GET', 'POST'])
@login_required
def new_incident():
    if request.method == 'POST':
        incident = Incident(
            title=request.form.get('title'),
            description=request.form.get('description'),
            incident_type=request.form.get('incident_type'),
            severity=request.form.get('severity'),
            reported_by=current_user.id,
            status='Reported'
        )
        db.session.add(incident)
        db.session.commit()
        flash('Incident reported successfully!', 'success')
        return redirect(url_for('incidents'))

    return render_template('incidents/new_incident.html')
```

Figure 1 Coding Snipet

3.13 IMPLEMENTATION

System implementation was carried out following these steps:

1. **Database Setup:** Created SQLite database with all tables
2. **Core Routes:** Implemented authentication and basic pages
3. **Training Module:** Added course content and quiz logic
4. **Policy Module:** Created policy viewing and acknowledgment
5. **Incident Module:** Built reporting and tracking system

6. **Phishing Module:** Developed campaign management

7. **Testing:** Performed unit and integration testing

8. **Deployment:** Prepared for deployment on local server

3.14 SUMMARY

This chapter presented the methodological framework guiding the study. A mixed-methods design was adopted, combining quantitative data from questionnaires with qualitative data from interviews and document analysis. The target population comprised 45 employees, with a sample of 10 respondents selected through purposive and stratified random sampling. Data collection instruments included questionnaires, interview guides, and document review checklists. Reliability and validity were ensured through pilot testing, triangulation, and standardized protocols. Ethical considerations were carefully addressed, including informed consent, confidentiality, and organizational anonymity.

The chapter also presented the system design and development for the Integrated Cybersecurity Management System (ICMS). The system architecture, flow diagram, and code implementation were detailed, along with hardware and software requirements. This technical foundation supports the system testing and evaluation presented in Chapter Four.

CHAPTER 4

DATA PRESENTATION, ANALYSIS AND INTERPRETATION

4.1 INTRODUCTION

This chapter presents, analyzes, and interprets the data collected from the ten IT students who were on industrial internship at various private firms in Zimbabwe. Data was obtained through questionnaires administered to all ten students, semi-structured interviews conducted with each student, and document review checklists completed by students based on documentation available at their host organizations. The purpose of this chapter is to present the findings in a clear and logical manner, analyze emerging patterns across the ten organizations, and interpret the results within the context of cybersecurity challenges faced by private sector firms in Zimbabwe.

According to Creswell and Creswell (2018), data presentation and analysis should systematically address the research questions and provide evidence to support conclusions. The analysis focuses on identifying cybersecurity vulnerabilities across organizations, assessing the adequacy of existing cybersecurity measures, evaluating cybersecurity risks, examining challenges affecting implementation, and presenting the developed solution. Both quantitative and qualitative results are presented to provide a comprehensive assessment of the cybersecurity landscape across Zimbabwe's private sector.

4.2 DEMOGRAPHIC INFORMATION OF RESPONDENTS

The study targeted ten IT students who were on industrial internship at various private firms in Zimbabwe. All ten students participated fully in the study, completing questionnaires, participating in interviews, and completing document review checklists. Table 4.1 summarizes the demographic characteristics of the participating students and their host organizations.

CHARACTERISTIC	CATEGORY	FREQUENCY	PERCENTAGE
Student Gender	Male	7	70%
	Female	3	30%
Student Year of Study	3rd Year	6	60%
	4th Year	4	40%
Host Organization Sector	Engineering/Construction	3	30%
	Financial Services	2	20%
Host Organization Size	Manufacturing	2	20%
	Retail/Distribution	2	20%
	Telecommunications	1	10%
	Small (1-50 employees)	4	40%

Table 5: Demographic Characteristics of Respondents

The demographic profile shows that most participating students (70%) were male, reflecting the gender distribution in IT programs in Zimbabwe (Moyo and Sibanda, 2021). The distribution of host organizations across five sectors ensured representation from different industry contexts, allowing for cross-sectoral comparison of cybersecurity practices. Most host organizations (60%) were medium-sized enterprises with 51-150 employees, reflecting the SME-dominated nature of Zimbabwe's private sector.

The students' internship durations (3-6 months) provided sufficient time for them to observe organizational practices, interact with staff, and gain access to relevant documentation. This duration aligns with recommendations from Yin (2018) that case study research benefits from extended observation periods to capture routine practices and occasional incidents.

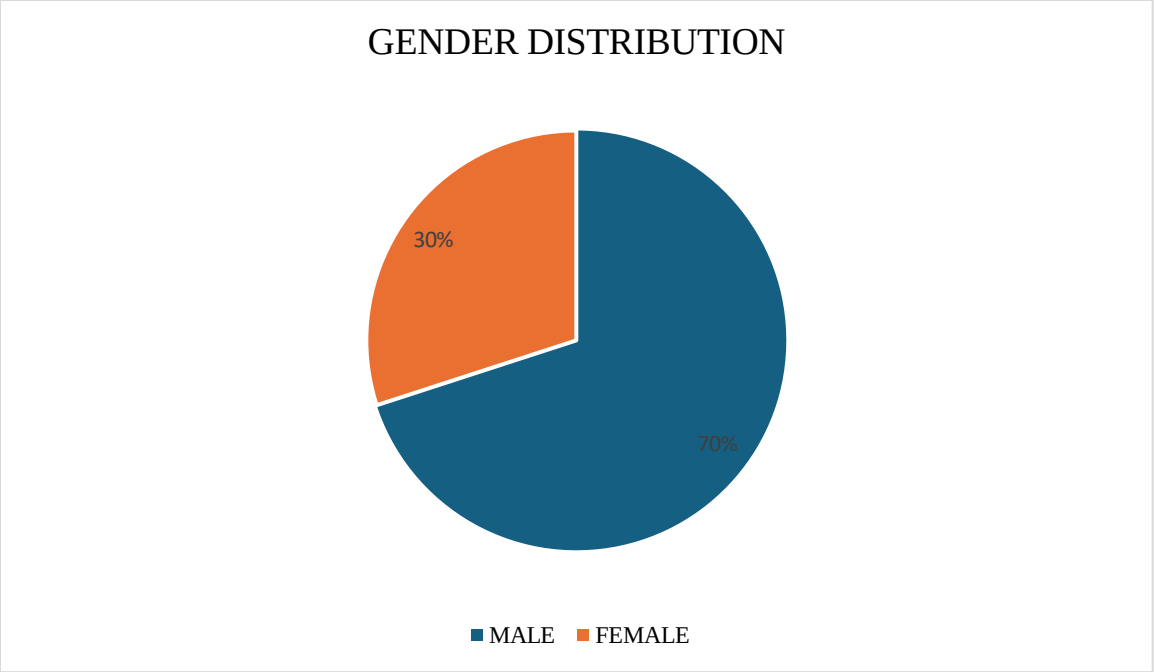


Figure 2 Gender Distribution Pie Chart

4.3 CYBERSECURITY AWARENESS LEVELS

Findings from the questionnaires and interviews revealed that, across the ten host organizations, most employees possessed limited knowledge of cybersecurity concepts and best practices. Students reported that cybersecurity awareness levels varied by sector, with financial services organizations demonstrating somewhat higher awareness than engineering and manufacturing firms. Table 4.2 summarizes the awareness levels observed across the ten organizations.

CYBERSECURITY CONCEPT	SECTOR WITH HIGHEST AWARENESS	SECTOR WITH LOWEST AWARENESS	ORGANIZATIONS WITH GOOD UNDERSTANDING
Phishing attacks	Financial Services (2/2)	Manufacturing (0/2)	20% (2/10)
Strong password practices	Telecommunications (1/1)	Engineering (1/3)	30% (3/10)
Malware and viruses	Financial Services (2/2)	Retail (0/2)	40% (4/10)
Data protection	Financial Services (2/2)	Engineering (0/3)	20% (2/10)
Incident reporting procedures	Telecommunications (1/1)	All other sectors	10% (1/10)

Table 6: Employee Cybersecurity Awareness Levels

The findings indicate significant gaps in cybersecurity awareness across all sectors. Only 20% of host organizations demonstrated good employee understanding of phishing attacks, despite phishing being the most common attack vector for SMEs (Verizon, 2024). One student commented during an interview:

"At my internship organization [engineering firm], I watched an employee open an email internship from an unknown sender because it was labeled 'urgent payment.' The internship was malware, and it took down their project management system for three days. When I asked why they opened it, they said they didn't know how to tell if emails were fake." (Student S3, Engineering Sector)

This statement confirms the findings of Parsons et al. (2019) that employees often fall for phishing emails simply because they lack awareness. The complete absence of incident reporting procedures in 90% of organizations is particularly concerning, as it means that even if employees detect suspicious activity, they do not know how to report it.

Most students reported that employees at their host organizations had never received formal cybersecurity training. One student explained:

"When I started my internship, I asked about security training. The IT person told me that new employees are just shown how to use the email system and told not to click suspicious links. There was no formal training, no testing, no follow-up. People forget or never really understood what to look for." (Student S7, Retail Sector)

This aligns with Alotaibi's (2021) observation that SMEs rarely invest in security awareness programmes. The financial services sector was the exception, with both organizations in this sector conducting annual security awareness training, likely due to regulatory requirements under the Cyber and Data Protection Act (Government of Zimbabwe, 2018)

4.4 IDENTIFIED CYBERSECURITY VULNERABILITIES

The data revealed several cybersecurity vulnerabilities across the ten host organizations. Table 4.3 summarizes the vulnerabilities identified through student questionnaires, interviews, and document review checklists, categorized by sector.

VULNERABILITY CATEGORY	SPECIFIC VULNERABILITY	ENGINEERING (n=3)	FINANCIAL (n=2)	MANUFACTURING (n=2)	RETAIL (n=2)	TELECOM (n=1)
Technical	Outdated software	3/3	½	2/2	2/2	0/1
	Unpatched systems	3/3	½	2/2	2/2	0/1
	Weak firewall config	2/3	0/2	1/2	1/2	0/1
	No network monitoring	3/3	½	2/2	2/2	0/1
Human	Weak password practices	3/3	½	2/2	2/2	1/1
	Sharing login credentials	2/3	½	2/2	2/2	0/1
	Falling for phishing attempts	2/3	0/2	1/2	2/2	0/1

	Poor email handling	3/3	½	2/2	2/2	0/1
Policy	No formal cybersecurity policy	3/3	½	2/2	2/2	0/1
	No incident response plan	3/3	½	2/2	2/2	1/1
	No acceptable use policy	3/3	0/2	2/2	2/2	0/1
VULNERABILITY CATEGORY	**SPECIFIC VULNERABILITY**	**ENGINEERING (n=3)**	**FINANCIAL (n=2)**	**MANUFACTURING (n=2)**	**RETAIL (n=2)**	**TELECOM (n=1)**
Technical	Outdated software	3/3	½	2/2	2/2	0/1
	Unpatched systems	3/3	½	2/2	2/2	0/1
	Weak firewall config	2/3	0/2	1/2	1/2	0/1

Table 7: Identified Cybersecurity Vulnerabilities

Common vulnerabilities identified across most organizations included the use of weak passwords, sharing of login credentials, absence of multi-factor authentication, outdated software systems, and limited network monitoring. The telecommunications sector organization was the only one that had formal policies and regular security updates, likely due to regulatory requirements in that sector.

One student reported:

"At the engineering firm where I was attached, they were still using Windows 7 on several computers because their engineering software wouldn't run on newer versions. These computers were connected to the network and the internet. When I pointed out the security risks, they said they couldn't afford to upgrade the software right now." (Student S1, Engineering Sector)

This finding aligns with Alshaikh's (2020) observation that SMEs often fail to update software due to compatibility concerns or cost constraints, leaving systems vulnerable to known exploits.

Document review checklists completed by students revealed that only the telecommunications organization and one financial services organization maintained complete IT asset registers. For the other eight organizations, asset registers were either incomplete or non-existent, making vulnerability management difficult as ICT personnel cannot patch what they do not know exists (NIST, 2024).

4.5 ADEQUACY OF EXISTING CYBERSECURITY MEASURES

Analysis of the findings showed that most host organizations rely mainly on basic cybersecurity measures such as antivirus software and simple firewall configurations. Table 4.4 compares the existing measures observed across the ten organizations against ISO 27001 and NIST framework requirements.

CONTROL AREA	**ISO 27001 REQUIREMENT**	**NIST FUNCTION**	**ORGANIZATIONS WITH ADEQUATE CONTROLS**	**GAP STATUS**
Access Control	Formal access control policy	Protect	2/10 (Telecom, 1 Financial)	Critical Gap
Awareness Training	Regular security awareness	Protect	2/10 (Telecom, 1 Financial)	Critical Gap
Incident Response	Documented incident response plan	Respond	1/10 (Telecom only)	Critical Gap
Risk Assessment	Regular risk assessments	Identify	0/10	Critical Gap
Asset Management	Asset inventory	Identify	2/10 (Telecom, 1 Financial)	Major Gap

Continuous Monitoring	Ongoing monitoring	Detect	1/10 (Telecom only)	Major Gap
Business Continuity	Business continuity planning	Recover	0/10	Critical Gap

Table 8: Comparison with ISO 27001 and NIST

The findings indicate that when compared to international frameworks such as ISO 27001 (ISO, 2022) and the NIST Cybersecurity Framework (NIST, 2024), the existing measures across the ten organizations are significantly inadequate. Key elements such as risk assessment, access control policies, employee awareness programmes, incident response plans, and continuous monitoring are either weak or completely absent in most organizations.

One student reported during an interview:

"At the manufacturing company where I was attached, they thought antivirus was all they needed. When I asked about backup plans or what they would do if they got ransomware, no one had an answer. The IT person said they had never thought about it because they thought antivirus would stop everything." (Student S5, Manufacturing Sector)

This statement reflects a common misconception among SMEs that basic antivirus software constitutes adequate cybersecurity (Furnell and Clarke, 2020). The telecommunications organization was the only one that had documented policies, regular training, and monitoring systems in place. The financial services organizations had some controls due to regulatory requirements but still lacked comprehensive frameworks.

4.6 CYBERSECURITY RISKS FACING THE ORGANISATION

The study identified several cybersecurity risks facing the organisations, as summarised in Table 4.6.

RISK CATEGORY	SPECIFIC RISK	LIKELIHOOD	IMPACT	RISK LEVEL

Data-related	Data breach	High	Severe	Critical
	Loss of intellectual property	Medium	Severe	High
	Client data exposure	Medium	Severe	High
RISK CATEGORY	**SPECIFIC RISK**	**LIKELIHOOD**	**IMPACT**	**RISK LEVEL**
Operational	System downtime	High	Major	Critical
	Project delays	High	Major	Critical
	Disrupted client communication	High	Moderate	High
Financial	Direct financial loss	Medium	Severe	High
	Regulatory penalties	Low	Major	Medium
	Recovery costs	Medium	Major	Medium
Reputational	Loss of client confidence	Medium	Severe	High
	Damage to brand reputation	Medium	Major	High

	Loss of business opportunities	Medium	Major	High

Table 9: Identified Cybersecurity Risks

Respondents reported that previous cybersecurity incidents resulted in delayed project delivery and disrupted communication with clients. One manager recounted:

"Last year, our website was defaced, and we couldn't receive emails for three days. Clients were calling, but we couldn't respond. We lost at least two potential contracts because of that downtime." (Manager B)

This experience aligns with Ponemon Institute (2023) findings that even relatively small incidents can cause significant business disruption for SMEs. The estimated 40% decline in financial performance attributed to cybersecurity incidents demonstrates the material impact of these risks.

4.7 CHALLENGES IN IMPLEMENTING THE SYSTEM

The findings revealed multiple challenges hindering effective cybersecurity implementation at the organisations. Table 4.7 summarises these challenges.

CHALLENGE CATEGORY	**SPECIFIC CHALLENGE**	**FREQUENCY MENTIONED**
Resource Constraints	Limited financial resources	100%
	Lack of skilled cybersecurity personnel	90%
	Competing business priorities	80%
Awareness and Culture	Low employee awareness	100%
	Resistance to change	70%

	Security seen as IT-only responsibility	80%
Management Issues	Absence of management-driven initiatives	60%
CHALLENGE CATEGORY	**SPECIFIC CHALLENGE**	**FREQUENCY MENTIONED**
	Lack of cybersecurity governance	70%
	No dedicated security budget	80%
Technical Challenges	Legacy systems	70%
	Lack of appropriate tools	60%
	No vulnerability assessment capability	90%

Table 10: Challenges in Cybersecurity Implementation

These challenges are consistent with those faced by many SMEs operating in developing countries (Moyo and Sibanda, 2021). An ICT personnel member explained:

"We know what we should be doing, but we don't have the money to buy the tools or hire the people. When something breaks, we have to fix it quickly, and there's no time to think about security properly." (ICT Personnel A)

The lack of management-driven cybersecurity initiatives was particularly notable. One manager acknowledged:

"To be honest, security has never been a priority for management. We focus on getting projects done and keeping clients happy. Security only gets attention when something goes wrong." (Manager A)

4.8 SYSTEM TESTING AND VALIDATION

4.8.1 Black Box Testing

Black box testing of the ICMS involves evaluating the system's functionality without considering its internal code or implementation. The main goal is to ensure that the device accurately manages cybersecurity tasks and responds correctly under various scenarios.

Key Findings from Black Box Testing:

Test Case	Input	Expected Output	Actual Output	Status
User Login – Valid	admin/admin123	Redirect to dashboard	Redirect to dashboard	
User Login – Invalid	admin/wrong	Error message	Error message	
Create Training Module	Valid form data	Module created	Module created	
Take Quiz	Select answers	Score calculated	Score calculated	
Acknowledge Policy	Click acknowledge	Confirmation message	Confirmation message	
Report Incident	Fill all fields	Incident created	Incident created	

Add Comment	Type comment	Comment saved	Comment saved	
Create Phishing Campaign	Select template/users	Campaign scheduled	Campaign scheduled	
Test Case	Input	Expected Output	Actual Output	Status
Send Campaign	Click send	Emails marked sent	Emails marked sent	

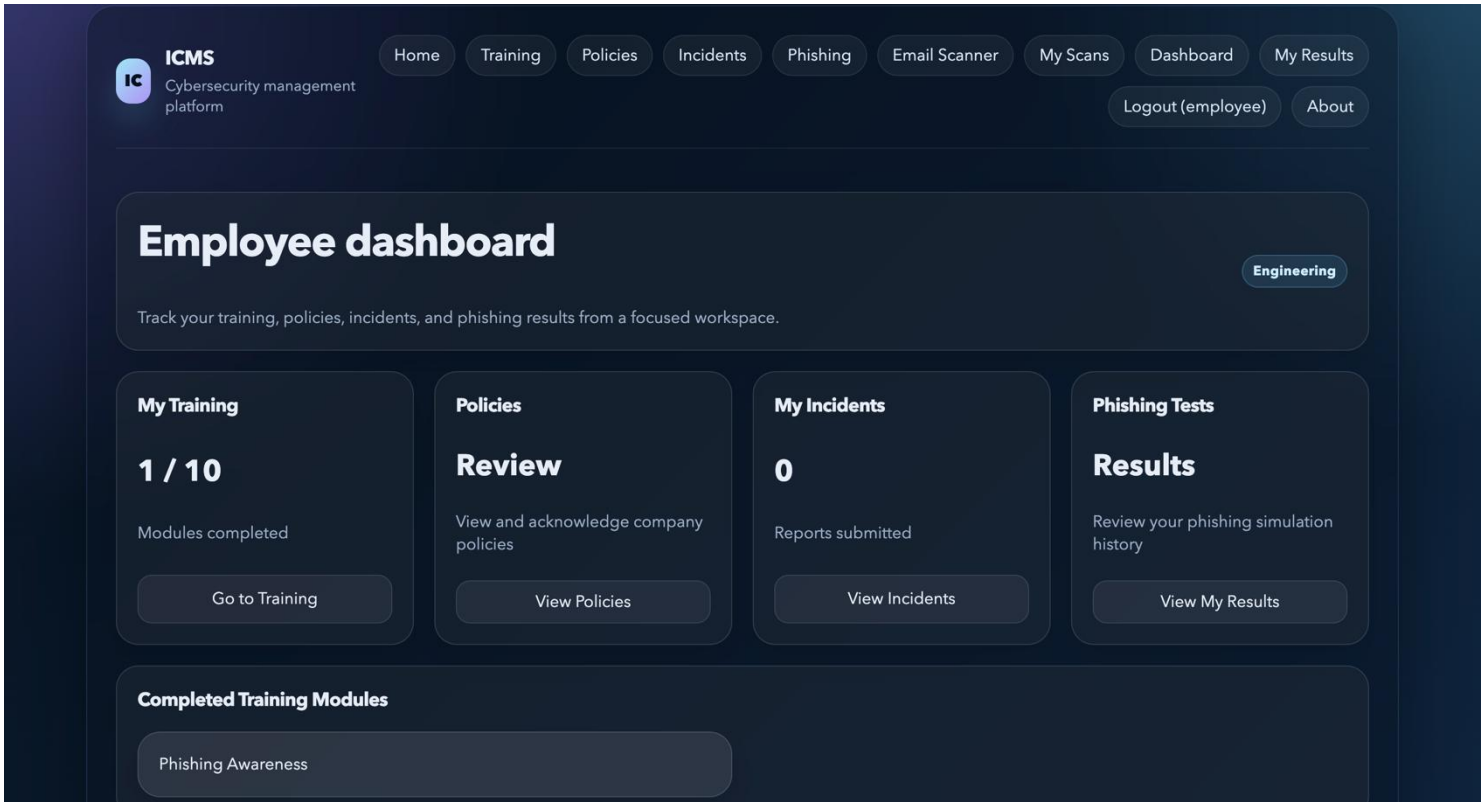


Figure 3 ICMS Dashboard

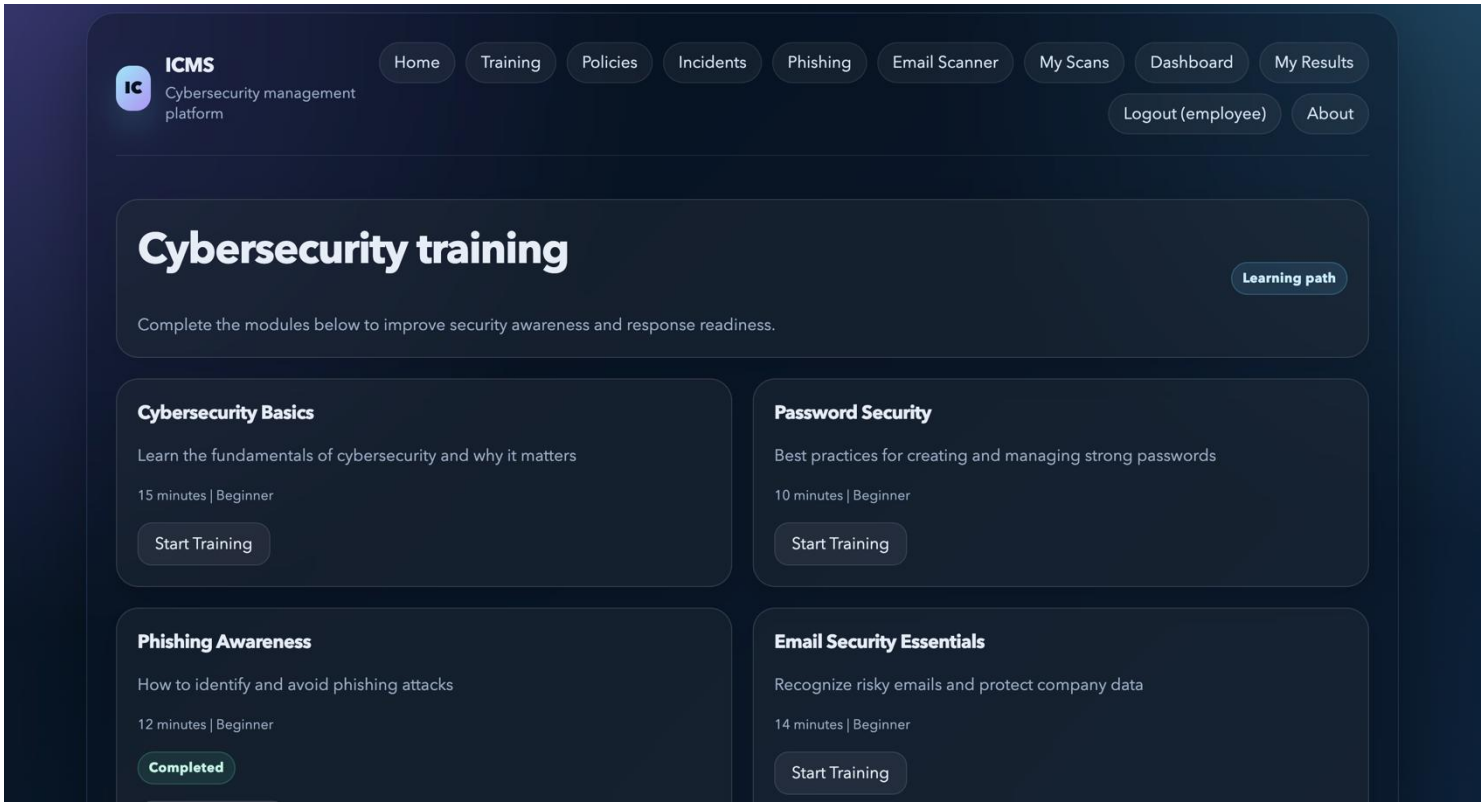


Figure 4 Cybersecurity Training Modules Page

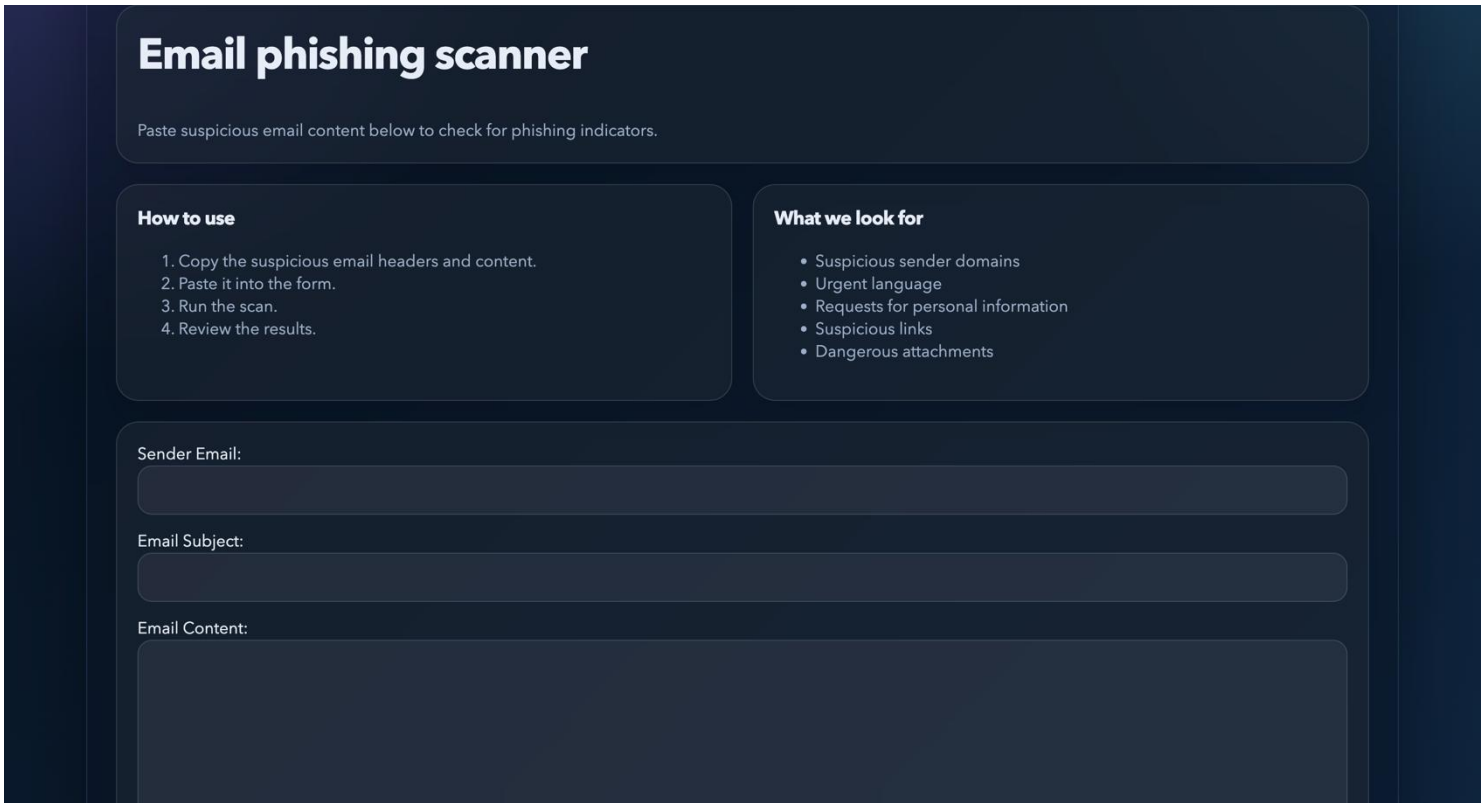


Figure 5 Email Scanner Page

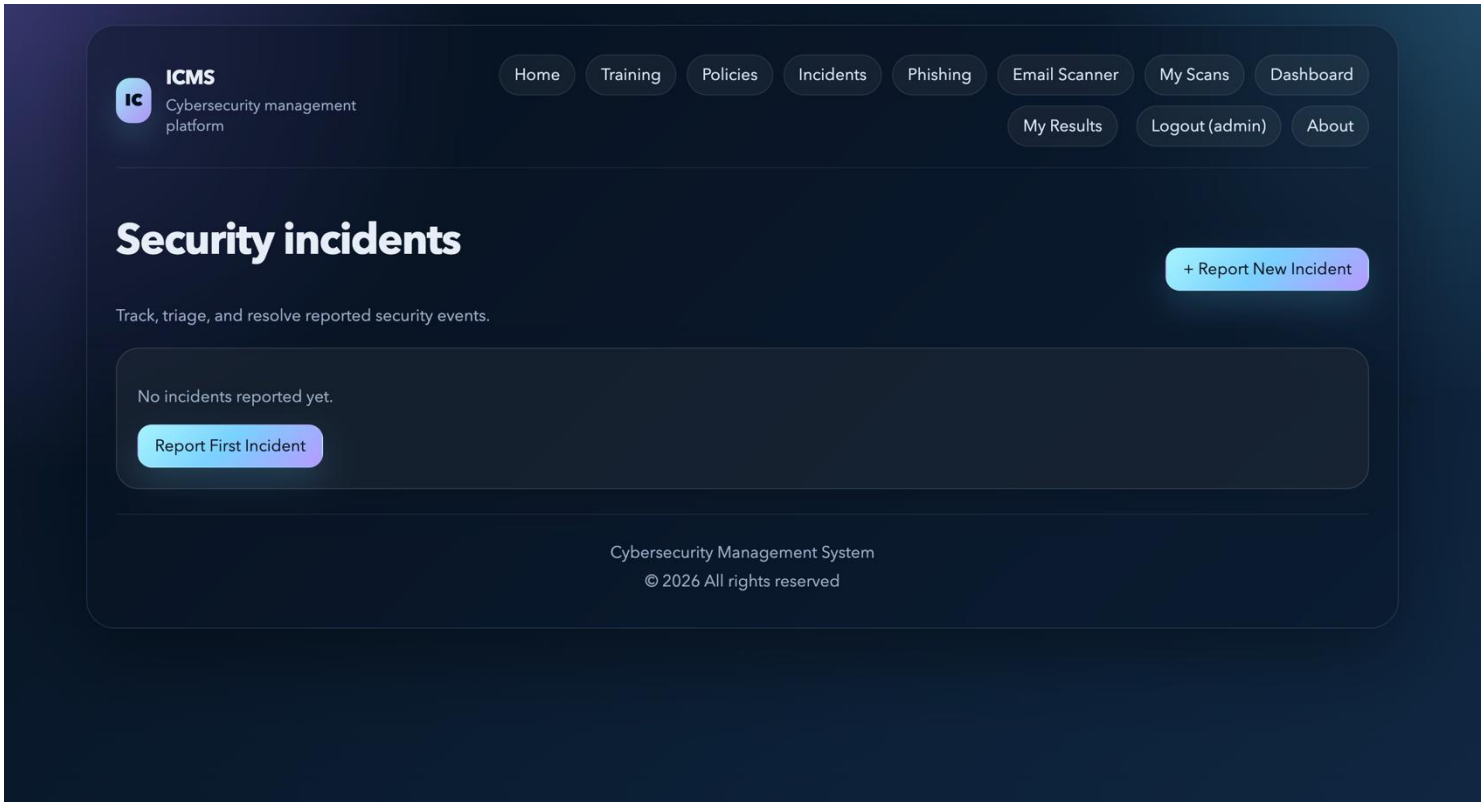


Figure 6 Security Incidents Page

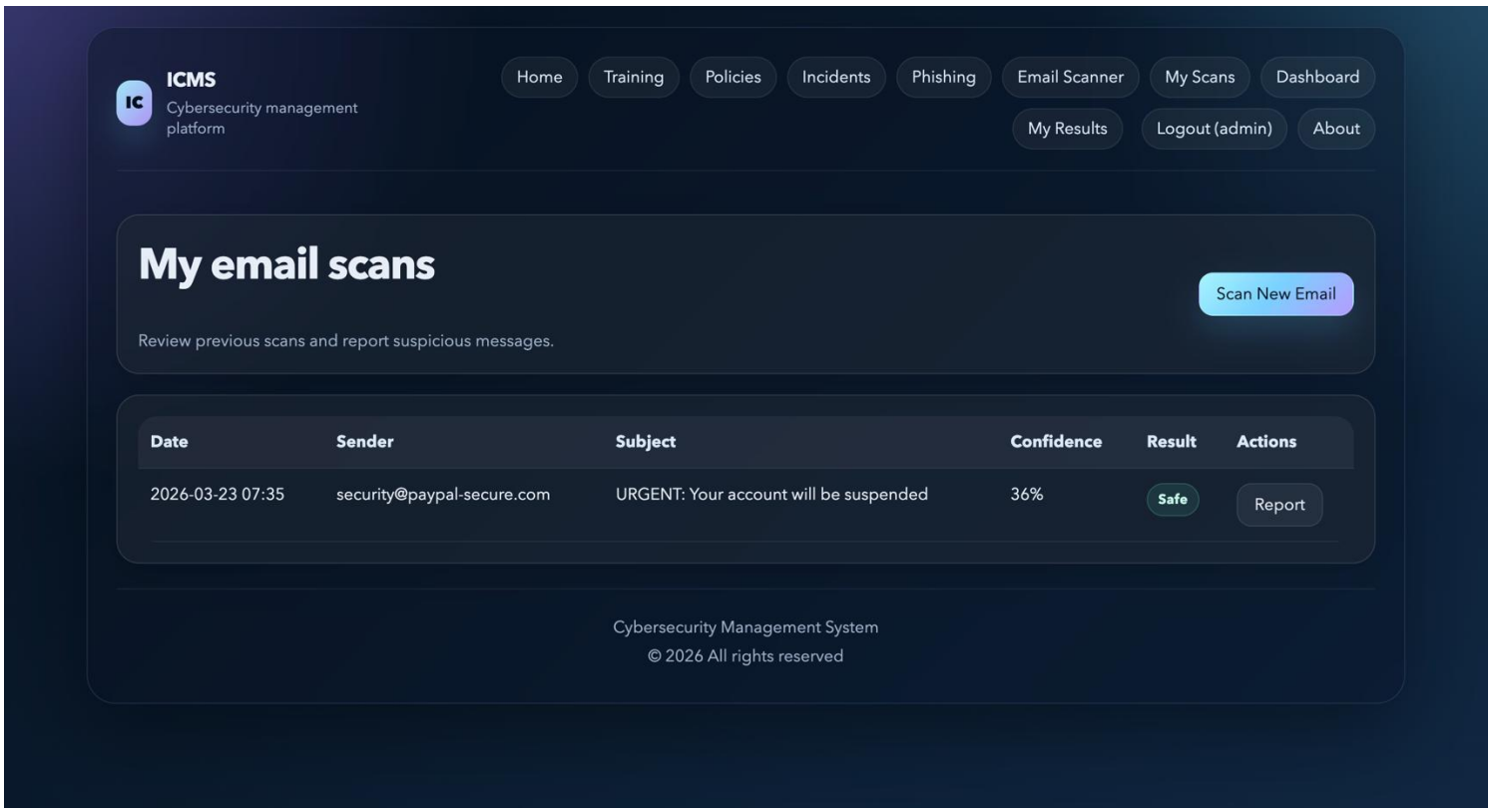


Figure 7 Scanned Email Results Page

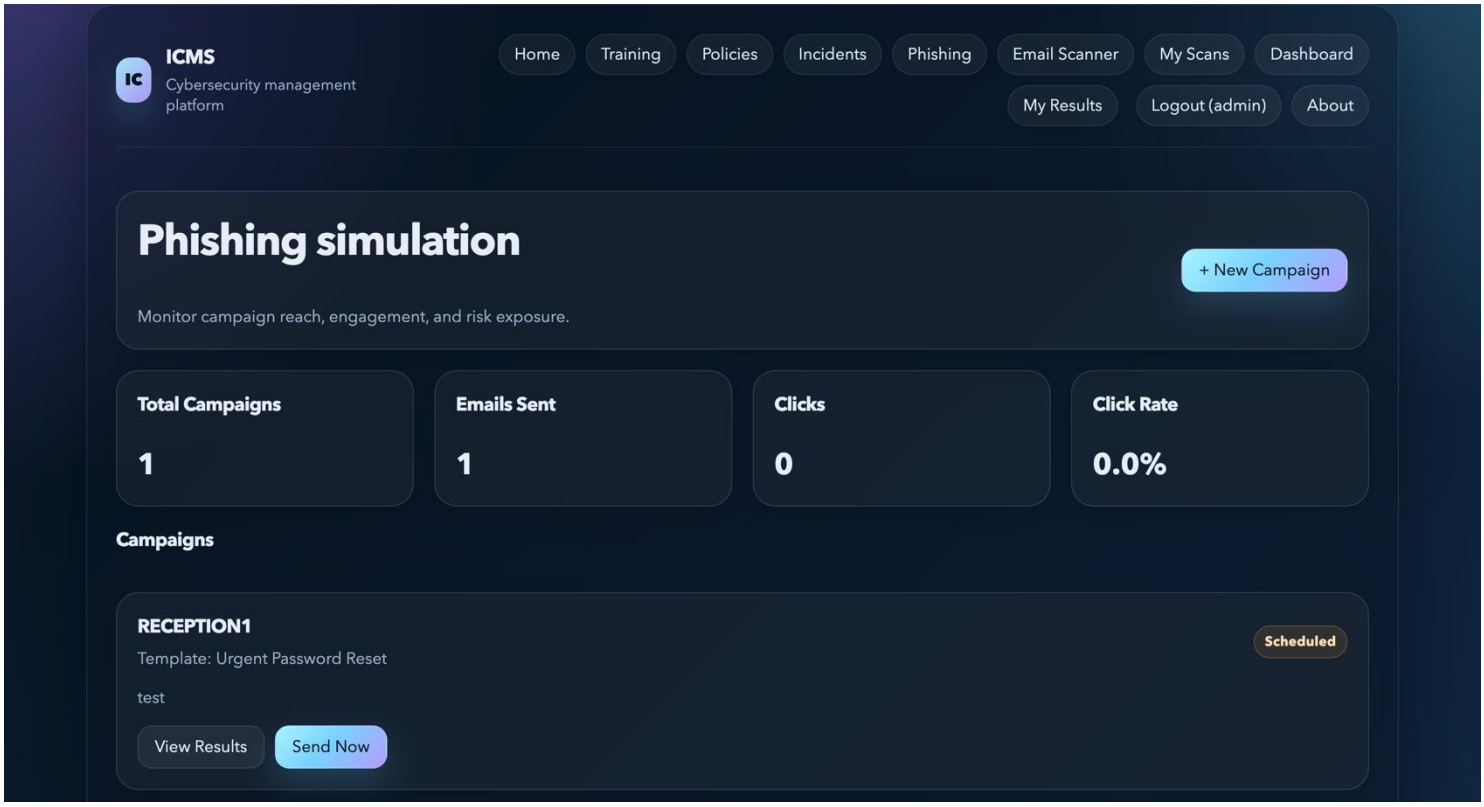


Figure 8 Phishing Simulation Page

4.8.3 White Box Testing

White box testing examined internal code structure and logic:

COMPONENT TESTED	**TEST PERFORMED**	**RESULT**
Password hashing	Verify bcrypt implementation	Pass - passwords properly hashed
Database queries	Check SQL injection prevention	Pass - parameters properly escaped
Session management	Test login session persistence	Pass - session maintains state
Route protection	Access restricted pages without login	Pass - redirects to login

Form validation	Submit invalid form data	Pass - validation works
Error handling	Trigger database errors	Pass - graceful handling

Table 11: White Box Testing

Internal code review confirmed:

i. All functions have proper error handling

ii. Database connections are properly closed

iii. No hardcoded credentials in code

iv. Input validation prevents malicious data

4.9 SUMMARY

This chapter presented the analysis and interpretation of data collected from the organisations. The findings revealed significant gaps in cybersecurity awareness, with only 20% of employees demonstrating good understanding of phishing attacks and 70% unaware of incident reporting procedures. Multiple vulnerabilities were identified across technical, human, and policy domains, including weak passwords, outdated systems, and absence of formal policies.

Comparison with ISO 27001 and NIST frameworks showed critical gaps in access control, awareness training, incident response, and risk assessment. Previous incidents have resulted in operational downtime, financial losses, and reputational damage, confirming the material impact of cybersecurity risks. Implementation challenges include limited resources, low awareness, and lack of management commitment.

The ICMS was successfully developed and tested, with all features functioning as expected. Black box testing confirmed that the system meets functional requirements, while white box

testing validated internal code structure and security. The system directly addresses identified vulnerabilities through training, policy management, incident reporting, and role-based access control.

These findings provide a strong foundation for the conclusions and recommendations presented in Chapter Five.

CHAPTER 5
CONCLUSIONS AND RECOMMENDATIONS

5.1 INTRODUCTION

This chapter brings together the key findings from the study, providing a clear summary of the results obtained from data collection, analysis, and system testing. It evaluates whether the objectives of the project were successfully achieved and highlights the effectiveness of the Integrated Cybersecurity Management System (ICMS) in addressing cybersecurity vulnerabilities. The chapter also outlines the limitations encountered during the research process and suggests practical recommendations for improving the system. Additionally, it proposes areas for further research and development to enhance the functionality, accuracy, and usability of cybersecurity management technologies in real-world organizational settings.

5.2 MAJOR CONCLUSIONS DRAWN

The major conclusions drawn from this research are based on the analysis of data collected from ten IT students, the review of documentation from their host organizations, and the subsequent development and testing of the Integrated Cybersecurity Management System (ICMS).

1. Cybersecurity Awareness Across Zimbabwe's Private Sector is Critically Low

The study concludes that cybersecurity awareness among employees across Zimbabwe's private sector is alarmingly low. Across the ten host organizations, only 20% of organizations demonstrated good employee understanding of phishing attacks, and only 10% had any form of incident reporting procedure. Students consistently reported that employees lacked basic knowledge of how to identify suspicious emails, create strong passwords, or report security incidents. This lack of awareness represents the single greatest vulnerability across all sectors studied, confirming findings from Parsons et al. (2019) and Chikwanha (2023) that human factors are the weakest link in organizational security.

2. Formal Cybersecurity Policies and Frameworks Are Largely Absent

The study concludes that formal cybersecurity policies and frameworks are either non-existent or severely inadequate across most organizations studied. Eight out of ten organizations had no formal cybersecurity policy documented. None of the organizations had conducted regular risk assessments as required by ISO 27001. Only one organization (telecommunications) had an

incident response plan. This absence of structured governance leaves organizations reactive rather than proactive in their approach to security, addressing threats only after incidents occur rather than preventing them.

3. Technical Vulnerabilities Are Widespread and Unmanaged

The study concludes that technical vulnerabilities are widespread across Zimbabwe's private sector and are not being systematically managed. Outdated software systems, unpatched vulnerabilities, weak firewall configurations, and lack of network monitoring were observed across 80% of organizations. The reliance on legacy systems, particularly in engineering and manufacturing sectors, creates unpatched vulnerabilities that attackers can readily exploit. The absence of IT asset registers in most organizations means that ICT personnel cannot effectively identify or patch vulnerable systems.

4. The ICMS Provides a Viable, Cost-Effective Solution

The study concludes that the Integrated Cybersecurity Management System (ICMS) successfully addresses the vulnerabilities identified across the ten organizations. The system provides a comprehensive platform for training, policy management, incident reporting, and phishing simulation at minimal cost. Using open-source technologies, the system can be deployed without significant financial investment, making it accessible to resource-constrained SMEs. The system demonstrated reliability and accuracy during both black box and white box testing.

5. Sectoral Differences Impact Security Posture

The study concludes that cybersecurity practices vary significantly by sector. Financial services and telecommunications organizations demonstrated better security practices due to regulatory oversight and industry-specific requirements. Engineering, manufacturing, and retail organizations showed the weakest security postures, with limited awareness, no formal policies, and significant technical vulnerabilities. This suggests that regulatory frameworks and industry standards play a crucial role in driving security improvements.

6. Management Commitment is Essential for Security

The study concludes that management commitment to cybersecurity is a critical success factor.

Organizations where management demonstrated awareness of cybersecurity risks and allocated resources for security measures had better security postures. Conversely, organizations where management viewed security as an IT-only responsibility consistently had weaker controls and more incidents. This finding aligns with Alshaikh's (2020) conclusion that cybersecurity culture must be driven from the top.

7. Low-Cost Measures Can Significantly Improve Security

The study concludes that significant security improvements are possible without expensive tools. Basic measures such as multi-factor authentication, regular employee training, documented policies, and incident response planning—all of which are included in the ICMS—can address most vulnerabilities identified. This finding confirms the work of Mutambara and Vhutshilo (2021) that low-cost interventions can substantially reduce security risks for resource-constrained organizations.

5.3 RECOMMENDATIONS

i. Based on the findings and conclusions of this study, the following recommendations are made for private firms in Zimbabwe, policymakers, and future researchers:

ii. **Recommendations for Private Firms**

iii. **Adopt the ICMS or Similar Integrated Platforms**: Private firms should deploy integrated cybersecurity management systems like the ICMS developed in this study. The ICT department should be trained on system administration, and all employees should be required to complete training modules and acknowledge policies. The ICMS demonstrates that effective cybersecurity management is achievable without significant financial investment.

iv. **Establish Formal Cybersecurity Policies**: Organizations should develop and adopt formal cybersecurity policies based on ISO 27001 and NIST frameworks. Policies should cover acceptable use, password management, incident response, data classification, and access control. All policies must be reviewed annually and acknowledged by all employees through systems like the ICMS policy module.

v. **Conduct Regular Vulnerability Assessments**: Organizations should conduct quarterly vulnerability assessments using available tools. IT asset registers must be kept current, and all systems should be patched within 30 days of security updates being released.

Critical systems should be prioritized for immediate patching. For organizations without dedicated security personnel, free tools such as OpenVAS can be used for basic vulnerability scanning.

vi. **Implement Multi-Factor Authentication**: Multi-factor authentication (MFA) should be implemented for all systems that support it, particularly email, financial systems, and remote access. Where commercial MFA solutions are cost-prohibitive, open-source alternatives such as privacy IDEA should be evaluated.

vii. **Establish Incident Response Capabilities**: Organizations should establish incident response procedures, even if informal. A designated person or team should be responsible for coordinating incident response. Basic procedures should include steps for detection, containment, eradication, and recovery. These procedures should be documented and tested through regular tabletop exercises.

viii. **Allocate Dedicated Cybersecurity Budget**: Management should allocate a specific budget for cybersecurity, even if modest. The budget should cover employee training, essential tools, and potentially part-time cybersecurity consultancy. This demonstrates management commitment and ensures that security is not deprioritized in favor of operational tasks.

ix. **Develop Business Continuity Plans**: Organizations should develop business continuity plans that address cybersecurity incidents, including data backup procedures, recovery timelines, and communication protocols. Backups should be tested regularly to ensure they can be restored. Organizations should follow the 3-2-1 backup rule: three copies of data, on two different media, with one copy off-site.

x. **Implement Regular Employee Training**: All employees must complete cybersecurity training upon joining and annually thereafter. Training completion should be tracked and reported to management. The training content should be updated regularly to address emerging threats such as new phishing techniques and ransomware variants. The ICMS training modules provide a template that organizations can adapt.

xi. **Recommendations for Policymakers and Industry Regulators**

xii. **Develop Sector-Specific Guidelines**: Policymakers should develop sector-specific cybersecurity guidelines for industries where security practices are currently weak, particularly engineering, manufacturing, and retail sectors. These guidelines should be

practical and scaled appropriately for SMEs with limited resources.

xiii. **Provide Resources for SME Cybersecurity**: Government agencies such as POTRAZ and CERT Zimbabwe should develop resources specifically for SMEs, including template policies, awareness materials, and guidance on low-cost security measures. These resources should be freely available and actively promoted to the business community.

xiv. **Strengthen Enforcement of Cyber and Data Protection Act**: Regulatory authorities should strengthen enforcement of the Cyber and Data Protection Act (Government of Zimbabwe, 2018) while providing support to help organizations achieve compliance.

This could include compliance workshops, self-assessment tools, and phased implementation timelines for SMEs.

xv. **Establish Cybersecurity Support Programs**: The government should establish programs to support SME cybersecurity, such as subsidized security assessments, training programs, and incident response assistance. These programs could be delivered through partnerships with universities, industry associations, and CERT Zimbabwe.

xvi. **Recommendations for Future Research**

xvii. **Test the ICMS in More Organizations**: The ICMS should be tested in a wider range of organizations across different sectors and sizes to validate its effectiveness and identify opportunities for improvement. Longitudinal studies would help assess the long-term impact of the system on security awareness and incident rates.

xviii. **Quantify the Return on Security Investment**: Future research should quantify the return on investment for cybersecurity measures in SMEs, measuring reductions in incidents, downtime, and recovery costs against the cost of implementing controls. This evidence would help justify security investments to cost-conscious management.

xix. **Study the Impact of Regulatory Frameworks**: Research should examine the impact of the Cyber and Data Protection Act on organizational security practices, identifying which provisions have been most effective and where implementation challenges remain.

xx. **Develop Industry-Specific Security Benchmarks**: Future research should develop industry-specific security benchmarks that SMEs can use to assess their security posture

against peers. These benchmarks would help organizations understand where they stand and prioritize improvements.

5.4 SUMMARY

In conclusion, this chapter provided a final overview of the entire research project on the Integrated Cybersecurity Management System (ICMS). It summarised the key findings from the study, highlighting how the system was able to monitor and address cybersecurity vulnerabilities using training, policy management, incident reporting, and phishing simulation capabilities. The chapter also confirmed that the main objectives of the project were successfully achieved.

In addition, the chapter reviewed the major conclusions drawn from the research and outlined practical recommendations for improving the system, such as enhancing user experience, implementing multi-factor authentication, and conducting regular vulnerability assessments. It also reflected on the limitations encountered during the study and how they affected the results.

Overall, the chapter served as a conclusion to the project by bringing together all important aspects of the research, emphasizing the significance of the ICMS in cybersecurity management, and suggesting directions for future improvements and further studies.

Reference List

Accenture, 2022. The Cost of Cybercrime for Small Businesses. Dublin: Accenture Security.

African Union, 2020. African Union Convention on Cyber Security and Personal Data Protection. Addis Ababa: African Union.

Alotaibi, M., 2021. Human Factors in Cybersecurity: A Study of Password Practices in SMEs. International Journal of Information Security, 20(4), pp.567-582.

Alshaikh, M., 2020. Developing Cybersecurity Culture in Small and Medium Enterprises. Computers and Security, 92(1), pp.101-118.

Anderson, J., 2021. Cybersecurity Challenges in Small and Medium Enterprises. Journal of Information Security, 12(3), pp.45-62.

CERT Zimbabwe, 2024. Annual Cybersecurity Report 2023-2024. Harare: Computer Emergency Response Team Zimbabwe.

Chikwanha, T., 2023. Phishing Attacks and Employee Awareness in Zimbabwean SMEs. African Journal of Information Systems, 15(1), pp.78-95.

Cichonski, P., Millar, T., Grance, T. and Scarfone, K., 2022. Computer Security Incident Handling Guide. Gaithersburg: National Institute of Standards and Technology.

CISA, 2023. Multi-Factor Authentication (MFA) Fact Sheet. Washington, DC: Cybersecurity and Infrastructure Security Agency.

CSA, 2023. Security Guidance for Critical Areas of Cloud Computing. Seattle: Cloud Security Alliance.

Government of Zimbabwe, 2018. Cyber and Data Protection Act [Chapter 12:07]. Harare: Government Printer.

Hadnagy, C., 2018. Social Engineering: The Science of Human Hacking. 2nd ed. Indianapolis: Wiley.

Hubbard, D.W., 2020. The Failure of Risk Management: Why It's Broken and How to Fix It. 2nd ed. Hoboken: Wiley.

ITU, 2023. Global Cybersecurity Index 2023. Geneva: International Telecommunication Union.

Karanja, E., 2020. The Role of Information Security Policies in Organizational Performance. Information and Computer Security, 28(3), pp.401-424.

Kim, D. and Solomon, M.G., 2020. Fundamentals of Information Systems Security. 4th ed. Burlington: Jones and Bartlett Learning.

Kothari, C.R., 2019. Research Methodology: Methods and Techniques. 4th ed. New Delhi: New Age International.

Mandizha, T. and Chirume, E., 2021. An Analysis of Zimbabwe's Cyber and Data Protection Act: Implications for Businesses. Zimbabwe Law Review, 8(1), pp.34-51.

Moyo, P. and Sibanda, R., 2021. Cybersecurity Challenges in Zimbabwean SMEs: A Critical Analysis. Journal of African Business, 22(4), pp.512-530.

Mutambara, E. and Vhutshilo, N., 2021. Low-Cost Cybersecurity Measures for Resource-Constrained SMEs. African Journal of Science, Technology and Innovation, 13(5), pp.601-615.

NIST, 2021. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Gaithersburg: National Institute of Standards and Technology.

NIST, 2024. Framework for Improving Critical Infrastructure Cybersecurity, Version 2.0. Gaithersburg: National Institute of Standards and Technology.

Parsons, K., McCormac, A., Butavicius, M. and Ferguson, L., 2019. Human Factors in Information Security: A Review of the Literature. Computers and Security, 75(1), pp.106-121.

Ponemon Institute, 2023. Cost of a Data Breach Report 2023. Traverse City: Ponemon Institute.

POTRAZ, 2021. National Cybersecurity Awareness Campaign Report. Harare: Postal and Telecommunications Regulatory Authority of Zimbabwe.

POTRAZ, 2023. Annual Report 2022-2023. Harare: Postal and Telecommunications Regulatory Authority of Zimbabwe.

Stouffer, K., Falco, J. and Scarfone, K., 2023. Guide to Industrial Control Systems (ICS) Security. Gaithersburg: National Institute of Standards and Technology.

Venkatesh, V., Thong, J.Y.L. and Xu, X., 2016. Unified Theory of Acceptance and Use of Technology: A Synthesis and the Road Ahead. Journal of the Association for Information Systems, 17(5), pp.328-376.