Cape Peninsula University of Technology

# An Awareness Model for the Use of Information Technology Security Policies in the Petroleum Retail Sector in South Africa

**by**

**Zandiswa Nkandi**

**Submitted in fulfilment of the requirements for the degree**

**MASTER OF TECHNOLOGY: INFORMATION TECHNOLOGY**

**in the faculty of Informatics and Design**

**to be awarded at Cape Peninsula University of Technology**

**Supervisor: Professor Ephias Ruhode**

**Cape Town**

**November 2023**

CPUT copyright information

The dissertation may not be published either in part (in scholarly, scientific, or technical journals) or as a whole (as a monograph) unless permission has been obtained from the University.

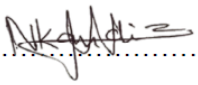
## DECLARATION

I, Zandiswa Nkandi, hereby declare that:

The work contained in this dissertation/thesis is my own work.

All sources or references have been documented and acknowledged.

This dissertation has never before been submitted, or has it been utilized before to partially fulfil the requirements for a qualification that is equivalent to or higher at another recognized academic institution.

Signature 

Date .....11 November 2023

## ABSTRACT

The petroleum (oil and gas) retail industry in South Africa depends on the use of Information Technology (IT) in its operations, including distribution. Consequently, digital transformation has become a necessity in order to improve quality, productivity and efficiency and mitigate the emergence of Information Technology security (IT security) related vulnerabilities and threats. As a result, this study investigates an awareness model for the use of information technology policies in the petroleum retail sector in South Africa. In essence, it has become imperative to ensure that the South African oil and gas industry's reliance on IT technology is safeguarded and efficient protocols are identified in order to strengthen security and compliance in the petroleum industry in its use of IT. This study uses a mono-quantitative research methodology and a non-probability purposive sampling technique. The data sources for this study were IT managers and non-managerial managers and employees within the IT units. Data analysis was performed using the statistical software SPSS. In this study, it was observed that there are disparities in adherence to access management techniques in order to secure vulnerable IT infrastructures and prevent cybersecurity threats. Also, the results from this study showed that approximately 89% agreed to the use of strong authentication methods, and 92% were favourable to the use of multi-factor authentication procedures, such as the adoption of password and SMS code protocols to be enforced among staff of the targeted oil and gas retail industry. The findings on knowledge, security, training approach, data sharing, and compliance represent the level of awareness of cybersecurity protection strategies, the need for frequent training, and data sharing among different categories of people were some of the observed to be among the control measures, organisational factors and challenges associated with cybersecurity within the oil and gas retail industry. This study reveals that a holistic measure must be developed as an IT security framework to mitigate against the cyber security of vulnerable operations within the oil and gas industry.

**Keywords**

Cybersecurity, IT security controls; IT security policies, Insider threats, IT security awareness, IT Security Compliance, IT Security Adoption

## ACKNOWLEDGEMENTS

This study's successful outcome is due to the numerous individuals who made various contributions. My supervisor, Professor Ephias Ruhode of the Faculty of Informatics and Design Systems in the Information Technology Department at the Cape Peninsula University of Technology, deserves a great deal of gratitude from me for his insightful and helpful criticism, which greatly aided in the completion of my thesis.

Prof. Ephias Ruhode, I appreciate you holding my hand through this exhausting, hard, but gratifying academic path. I am honoured to stand here and pay respect to your tremendous mentorship, direction, and desire to achieve an outcome you are happy with today.

I would like to express my gratitude to my employer for providing me with the necessary resources as well as the motivation to successfully complete this journey.

I also want to thank my pastor, close friends and co-workers, who have been there for me throughout this study. I appreciate all of the feedback and suggestions that you have provided. I am indebted to each and every one of you for your kindness.

## DEDICATION

To the Divine Source of Wisdom and Guidance

This thesis is sincerely dedicated to God, the supreme source of wisdom and comprehension. During this journey of research and discovery, I am struck with tribute for the abundant knowledge and kindness that have enlightened my way. God's brilliant light has illuminated my path forward during periods of uncertainty, and His strength has sustained me during times of difficulty. I dedicate this work as an expression of appreciation for God's direction and blessing on my academic endeavours.

It would be extremely unjust to disregard the support, encouragement and tolerance shown by my husband, James. My beloved children, Likhona and Joy, and my niece, Yola Lilitha, have served as my source of inspiration during this entire research process. There is no better way to dedicate this thesis than to each and every one of you.

In loving memory of my brother and sibling, Sanelisiwe Shura, whose joy and satisfaction at achieving this goal would be beyond words.

# TABLE OF CONTENTS

**DECLARATION** ..... **I**

**ABSTRACT** ..... **1**

**ACKNOWLEDGEMENTS** ..... **2**

**DEDICATION** ..... **3**

**TABLE OF CONTENTS** ..... **4**

**LIST OF FIGURES** ..... **8**

**LIST OF TABLES** ..... **9**

**LIST OF ANNEXURES** ..... **10**

**ACRONYMS** ..... **11**

**CHAPTER 1 INTRODUCTION AND BACKGROUND** ..... **13**

1.1 PREAMBLE ..... 13

1.2 INTRODUCTION ..... 13

1.3 BACKGROUND TO THE RESEARCH PROBLEM ..... 15

*1.3.1 Digital transformation and cybersecurity challenges in the petroleum retail sector ..... 15*

1.3.1.1 Internet of Things (IoT) devices ..... 29

1.3.1.2 Artificial Intelligence ..... 30

1.3.1.3 Cloud-Based Systems ..... 31

1.3.1.4 Interconnected Networks ..... 33

*1.3.2 Impact of cybersecurity incidents ..... 16*

*1.3.3 Importance of information technology security policies ..... 16*

*1.3.4 Global and local cyber security regulatory compliance ..... 18*

*1.3.5 Employee training and cybersecurity culture ..... 19*

1.4 SIGNIFICANCE OF THE RESEARCH STUDY ..... 20

1.5 PROBLEM STATEMENT ..... 21

1.6 RESEARCH QUESTIONS ..... 22

1.7 RESEARCH OBJECTIVES ..... 23

1.8 DELINEATION OF THE RESEARCH ..... 23

1.9 STRUCTURE OF THESIS ..... 24

1.10 CHAPTER SUMMARY ..... 25

**CHAPTER 2 LITERATURE REVIEW ..... 27**

2.1 INTRODUCTION ..... 27
2.2 EMPIRICAL CASE ..... 27
2.3 CYBERSECURITY ..... 28
*2.3.1 Social engineering attacks ..... 34*
2.3.1.1 The physical element of social engineering ..... 35
2.3.1.2 The technical element of social engineering ..... 36
2.3.1.3 The psychological element of social engineering ..... 37
*2.3.2 Safeguarding cybersecurity using control types ..... 42*
*2.3.3 Prevention, detection, and response against cybersecurity ..... 42*
*2.3.4 Cybersecurity culture ..... 46*
2.3.4.1 Organisational climate ..... 47
2.3.4.2 Management support, leadership, or involvement ..... 47
*2.3.5 Cybersecurity body of knowledge ..... 49*
*2.3.6 Insider threats ..... 53*
2.4 CHAPTER SUMMARY ..... 55

**CHAPTER 3 THEORETICAL FRAMEWORKS ..... 57**

3.1 INTRODUCTION ..... 57
3.2 DIFFUSION OF INNOVATION THEORY (DOI) ..... 57
3.3 SOCIAL COGNITIVE THEORY (SCT) ..... 59
3.4 TECHNOLOGY ACCEPTANCE MODEL (TAM) ..... 61
3.5 UNIFIED THEORY OF ACCEPTANCE AND USE OF TECHNOLOGY (UTAUT) ..... 63
3.6 TECHNOLOGY-ORGANISATION-ENVIRONMENT (TOE) ..... 64
*3.6.1 Background and context of TOE ..... 64*
*3.6.2 TOE Framework for IT Security Usage, Compliance and Adoption ..... 65*
*3.6.3 TOE Dimensions and Considerations ..... 66*
3.7 CHAPTER SUMMARY ..... 68

**CHAPTER 4 RESEARCH DESIGN AND METHODOLOGY ..... 70**

4.1 INTRODUCTION ..... 70
*4.1.1 The Research Philosophy ..... 71*
*4.1.2 Interpretivism paradigm ..... 71*
*4.1.3 Positivism paradigm ..... 71*
*4.1.4 Critical realism ..... 72*
4.2 APPROACH TO THEORY DEVELOPMENT ..... 73

4.3 Research Approach – Mono-Method Quantitative ..... 73
4.4 Research strategy and outcome ..... 75
4.5 Research time horizon ..... 76
4.6 Data collection ..... 77
4.7 Data analysis – Statistical Analysis ..... 79
4.8 Data Validation ..... 80
4.9 Sampling/justification ..... 80
4.10 Ethical considerations ..... 81
*4.10.1 Informed consent ..... 81*
*4.10.2 Anonymity and confidentiality ..... 82*
*4.10.3 Safety and respect ..... 82*
*4.10.4 Openness, Honesty and Trust ..... 82*
*4.10.5 Right to withdraw ..... 83*
4.11 Chapter Summary ..... 83

**CHAPTER 5 FINDINGS AND ANALYSIS ..... 84**

5.1 Introduction ..... 84
5.2 Access management ..... 85
5.3 Authentication ..... 119
5.4 Knowledge ..... 91
5.5 Security ..... 96
5.6 Training ..... 99
5.7 Data Sharing ..... 103
5.8 Compliance ..... 106
5.9 Chapter Summary ..... 111

**CHAPTER 6 DISCUSSION, CONCLUSION AND RECOMMENDATIONS ..... 113**

6.1 Introduction ..... 113
6.2 Discussion and implications of the findings ..... 113
6.3 Importance of further exploration ..... 115
6.4 Significance of the findings ..... 116
6.5 Contributions ..... 118
*6.5.1 Practical contributions ..... 118*
*6.5.2 Theoretical contributions ..... 119*
6.6 Limitations ..... 121
6.7 Recommendations ..... 122

6.8 CONCLUSION ..... 124
6.9 SUMMARY ..... 126

**REFERENCES ..... 127**

**ANNEXURES ..... 139**

## LIST OF FIGURES


FIGURE 1.1 THESIS STRUCTURE ..... 25
FIGURE 2.1 SOCIAL ENGINEERING ATTACKS ELEMENTS ..... 35
FIGURE 2.2 CYBERSECURITY AUTHORITY LEVELS ..... 49
FIGURE 2.3 CLASSIFICATION OF CYBOK KNOWLEDGE AREAS ..... 50
FIGURE 2.4 INSIDER THREATS AND COMPLIANCE BEHAVIOURS ..... 54
FIGURE 3.1 SOCIAL COGNITION THEORY ..... 60
FIGURE 3.2 TECHNOLOGY ACCEPTANCE MODEL (TAM) ..... 62
FIGURE 3.3 TOE FRAMEWORK ..... 66
FIGURE 4.1 RESEARCH ONION ..... 70
FIGURE 5.1 CLUSTER ANALYSIS ..... 86
FIGURE 5.2 UTILISING STRONG PASSWORD ..... 119
FIGURE 5.3 MFA METHODS ..... 119
FIGURE 5.4 VPN USAGE ..... 91
FIGURE 5.5 CORRELATIONS BETWEEN THE USE OF VPN AND ACCESS TO TRAINING ..... 92
FIGURE 5.6 CYBERSECURITY POLICY AWARENESS ..... 94
FIGURE 5.7 OBLIGATION TO LOG INCIDENTS ..... 94
FIGURE 5.8 CYBERSECURITY EXPECTATIONS ..... 95
FIGURE 5.9 INFORMATION ABOUT CYBERSECURITY ..... 95
FIGURE 5.10 REPORTING CYBERSECURITY QUESTIONS ..... 96
FIGURE 5.11 PREVIOUS CYBERATTACKS ..... 96
FIGURE 5.12 CORRELATIONS ON PREVIOUS ATTEMPTS VS HOME NETWORK/WI-FI ..... 97
FIGURE 5.13 CORRELATIONS ON PREVIOUS ATTEMPTS VS CYBERSECURITY EXPECTATIONS ..... 98
FIGURE 5.14 TRAINING FREQUENCY ..... 99
FIGURE 5.15 PARTICIPATION IN CYBERSECURITY TRAINING SESSIONS ..... 101
FIGURE 5.16 ACCESS TO TRAINING PLATFORM FOR CYBERSECURITY TOPICS ..... 102
FIGURE 5.17 DATA SHARING WITH EXTERNAL PARTIES ..... 103
FIGURE 5.18 DATA SHARING VIA SOCIAL MEDIA ..... 104
FIGURE 5.19 CORRELATIONS ON SHARING DATA VIA SOCIAL MEDIA AND WITH EXTERNAL PARTIES ..... 105
FIGURE 5.20 HACKING OR EXPLOITS ..... 106
FIGURE 5.21 NON-COMPLIANCE ACTIONS ..... 108
FIGURE 5.22 CLUSTERING ANALYSIS ..... 109

## LIST OF TABLES

TABLE 2.1 IT SECURITY CONTROLS ..... 45
TABLE 2.2 AN OUTLINE OF THE KNOWLEDGE AREAS ..... 51
TABLE 3.1 CONSIDERATIONS FOR TOE ..... 66
TABLE 4.1 RESEARCH QUESTIONS AND KEY OUTCOMES ..... 78

## LIST OF ANNEXURES

**ANNEXURE A: CONSENT TO PARTICIPATE IN STUDY** ..... 139
**ANNEXURE B: INTRODUCTORY LETTER FOR COLLECTION OF DATA** ..... 140
**ANNEXURE C: LETTER OF CONSENT -ENGEN** ..... 141
**ANNEXURE D: ETHICAL CLEARANCE** ..... 142
**ANNEXURE E: INTERVIEW QUESTIONNAIRE** ..... 143
**ANNEXURE F: INTERVIEW QUESTIONNAIRE DRAFT** ..... 146

## ACRONYMS

| Acronym | Full Name |
|---|---|
| **4IR** | Fourth Industrial Revolution |
| **AI** | Artificial Intelligence |
| **APT** | Advanced Persistent Threat |
| **CERTs** | Computer Emergency Response Teams |
| **CIIP** | Critical Information Infrastructure Protection |
| **CISA** | Cybersecurity Information Sharing Act |
| **CRM** | Customer Relationship Management |
| **DOI** | Diffusion of Innovation Theory |
| **ECTA** | The Electronic Communications and Transactions Act of 2002 |
| **ERP** | Enterprise Resource Planning |
| **IoT** | Internet of Things |
| **MAM** | Mobile Application Management |
| **MDM** | Mobile Device Management |
| **NCPF** | The National Cybersecurity Policy Framework |
| **NIST** | National Institute of Standards and Technology |
| **POPIA** | Protection of Personal Information Act |
| **SCT** | Social Cognitive Theory |
| **TAM** | Technology Acceptance Model |
| **TOE** | Technology-Organisation-Environment |
| **UTAUT** | Unified Theory of Acceptance and Use of Technology |

| | |
|---|---|
| **ISO/IEC 27001** | International Standard for Information Security |
| **CC** | International standard (ISO/IEC 15408) for computer security |

# CHAPTER 1
# INTRODUCTION AND BACKGROUND

## 1.1 Preamble

This section provides an overview of the topic under investigation. It describes the research topic, significance, and relevant trends or advancements. It provides the context for the specific research question or problem.

The chapter subsequently focuses on the specific research problem that the study intends to answer as well as the question/s and objective/s of the study.

## 1.2 Introduction

The Information Technology (IT) industry faces the challenge of evolving innovative technologies essential to business operations. These ever-changing technologies are presented by the Fourth Industrial Revolution (4IR). However, the emergence of innovative technologies poses potential vulnerabilities and threats associated with IT-dependent operations such as Inventory and Supply Chain Management, Manufacturing and Automation, Energy and Utilities Management, Data Storage and Backup Solutions, E-mail Communication, Customer Relationship Management (CRM) and Enterprise Resource Planning (ERP) that are used by various organisations including the Oil and Gas industry. As a result, there is a demand for stringent security measures to mitigate the potential threats and vulnerabilities of IT-dependent operations (Alghamdi, 2021).

Von Solms and von Solms (2018) define cybersecurity as the effort to safeguard an additional set of assets, namely human and organisational assets. These assets may be of significant value. This means that cyber security is not just about protecting hardware and software but also about safeguarding people and organisations from cyber threats. It is also about protecting the data and information of an organisation from malicious attackers. von Solms & von Solms (2018) further argue that cybersecurity is the same as information security, and information security is a part of cybersecurity.

The petroleum retail sector in South Africa has witnessed a significant transformation with the integration of information technology (IT), especially in its daily operations. The core responsibility of the petroleum retail sector is to distribute petroleum products. The responsibility requires an absolute dependence on IT systems for manufacturing and

distribution. The adoption of digital systems and processes has improved efficiency, enhanced customer experiences, and streamlined supply chain management. However, this rapid digitalisation has also exposed the sector to many cybersecurity threats, such as malware, phishing, ransomware, and advanced persistent threats, presenting substantial risks to accessing sensitive information and critical infrastructure (Stergiopoulos, Gritzalis & Limnaios, 2020).

The Oil and Gas industry operates several complex infrastructures, such as smart drilling technology and digital platforms for shipping (Ali, Dominic and Ali, 2020), and to safeguard against these escalating cyber threats, the implementation of robust information technology security policies becomes imperative (Ademola, 2019). Policies such as Network Security, Patch and Software Management, Password, Access Control, Encryption and Mobile Device Management (MDM) serve as a comprehensive framework, guiding organisations such as the petroleum retail sector in South Africa on how to protect their data, systems, and operations from malicious actors (Sharma & Garg, 2011). Developing and adhering to such policies is critical to maintaining customer trust, safeguarding corporate reputation, and ensuring the continued functioning of essential services provided by the sector.

This research study uses the current IT security landscape in the petroleum retail industry in South Africa to identify existing practices and difficulties faced by industry players. Furthermore, the investigation has studied the sector's specialised requirements, evaluating the important systems and data that require protection against cyber threats. Furthermore, the study has analysed relevant local and global rules governing IT security in the petroleum retail area, ensuring that the suggested model complies with both legal and industrial requirements.

This study focuses on an awareness model to promote the effective use, compliance and adoption of information technology security policies within the South African petroleum retail sector. By addressing this industry's unique challenges and requirements, the model aims to empower organisations to proactively mitigate potential cyber risks and respond efficiently to any security incidents that may arise.

In summary, this study aims to provide a valuable contribution to improving information technology security measures in the petroleum retail industry in South Africa by fostering

awareness, promoting compliance, and fostering a security-first mindset among organisation employees.

## 1.3 Background to the Research Problem

The petroleum retail industry in South Africa holds significant importance within the nation's economy. It accounted for 3.2% of the country's GDP and contributed R163 billion to the economy in 2019. The South African Industry Association (2019) and the South African oil industry serve as crucial suppliers of fuel and petroleum products to both consumers and diverse industrial sectors (Haouel & Nemeslaki, 2023). In recent years, the petroleum retail industry has witnessed notable gains in efficiency, inventory management, and customer experience due to the emergence of digitalisation and the integration of information technology (IT) into its operations (Parsoya & Perwej, 2021). In addition, several policies relating to cyber security, safety and secured digitalisation processes and operations have been introduced and implemented (Prostean et al., 2020).

Nevertheless, the growing dependence on information technology (IT) within the oil and gas sector has made it vulnerable to various cybersecurity risks. For instance, the dependence of the oil and gas sector on IT infrastructure has increased by approximately 50% since 2010. Consequently, this dependence has resulted in the potential to compromise the reliability and credibility of data, critical infrastructure and analytics employed in production processes (Armstrong Lee Agbaji, 2021).

### 1.3.1 Digital transformation and cybersecurity challenges in the petroleum retail sector

Over the past decade, the petroleum retail sector in South Africa has undergone a digital transformation by adopting advanced technologies such as automated fuel pumps, remote monitoring of equipment, predictive maintenance, electronic payment systems, cloud computing, real-time inventory tracking, remote sensing and satellite technology and customer loyalty programs, all of which have significantly improved the efficiency and competitiveness of the industry (Haouel & Nemeslaki, 2023).

Despite the numerous benefits of digitalisation, which include enhanced productivity, improved customer experience, supply chain optimisation, and improved efficiency and cost reduction, the petroleum retail sector faces a growing range of cybersecurity

challenges. As the global industry embraces Internet of Things (IoT) devices, Artificial Intelligence, cloud-based systems, and interconnected networks, it becomes increasingly vulnerable to cyber threats. Malicious, careless, and compromised actors, including hackers, cybercriminals, and state-sponsored entities, seek to exploit weaknesses in IT security through technology, insider, and infrastructure to gain unauthorised access to critical systems, steal sensitive information, disrupt operations, or cause financial harm (Wanasinghe et al., 2020).

### 1.3.2 Impact of cybersecurity incidents

The consequences of cybersecurity incidents in the petroleum retail sector can vary depending on the type of incidents. For instance, Jan et al. (2021) indicated that a successful cyberattack could be a national security threat, financial losses to corporate organisations, regulatory penalties, brand reputational damage, and potential legal liabilities. In addition, cyberattacks can disrupt supply chain mechanisms such that fuel supply or customer services can negatively impact consumers, businesses, and even national economic stability.

### 1.3.3 Importance of information technology security policies

IT security policies define formal instructions and guidelines that are documented to preserve information security within a business entity (Viegas & Kuyucu, 2022). Information security policies play a crucial role in safeguarding sensitive information and ensuring the overall security of an organisation's data and systems. These policies provide a structured framework to manage information security risks effectively and establish clear guidelines for employees and stakeholders. Information security policies contribute to protecting information by identifying potential threats and vulnerabilities that could compromise the confidentiality, integrity, or availability of information (Masrek et al., 2020).

South Africa has implemented various cybersecurity policies to address the escalating threat of cyberattacks and to safeguard critical information infrastructure, personal information, and national security. The following are notable cybersecurity policies and initiatives linked to the South African National Cybersecurity Policy Framework (Bote, 2019):

- **Protection of Personal Information Act (POPIA):** The Protection of Personal Information Act (POPIA) was implemented on July 1, 2020. The legislation governs the handling of personal data and puts specific obligations on entities to safeguard the privacy of persons' information.
- **Critical Information Infrastructure Protection Act 8 of 2019** South Africa has placed considerable emphasis on safeguarding critical infrastructure from cyber threats by implementing Critical Information Infrastructure Protection (CIIP) measures. The primary objective of the CIIP program is to ensure the protection and security of critical sectors such as energy, telecommunications, and finance.
- **Information Sharing and Incident Response:** Establishing national and regional Computer Emergency Response Teams (CERTs) is crucial for facilitating coordinated incident response and promoting effective information sharing. These teams have the ability to enhance the exchange of information and promote collaboration in the occurrence of cybersecurity incidents.
- **Resilience and Disaster Recovery:** Develop and implement strategies for enhancing the resilience of critical infrastructure and disaster recovery plans to minimise the impact of cyber incidents.
- **Awareness and Education:** Public awareness campaigns and educational initiatives can help raise awareness about the importance of cybersecurity among citizens, businesses, and government employees.
- **The Electronic Communications and Transactions Act of 2002 (ECTA)** was implemented in South Africa with the primary objective of establishing a legislative framework to regulate electronic communications and transactions. The legislation intends to address various aspects of the digital landscape, foster electronic commerce, and streamline the utilisation of electronic communications while safeguarding the security and reliability of these transactions.

In response to the amount of data handled by the petroleum retail sector and the escalating cybersecurity risks this industry is exposed to, implementing a robust information technology security framework that focuses on addressing insider threats is crucial for the petroleum retail sector in South Africa. The framework is essential for

establishing a secure and resilient information environment and providing a comprehensive guide to safeguard sensitive information and critical assets, uphold the organisation's reputation, and inspire confidence among customers, partners, and other organisational stakeholders.

### 1.3.4 Global and local cyber security regulatory compliance

Adherence to both local and global cybersecurity regulations is essential for organisations in the petroleum retail sector and other industries. By ensuring compliance, organisations can protect customer data, critical infrastructure, and reputation while mitigating cyber risks and maintaining a competitive edge in the marketplace. Failure to comply with these regulations can have serious consequences, underscoring the importance of prioritising cybersecurity and data protection in today's digital landscape.

There are several global and South African cyber security regulatory and compliance standards. The regulatory and compliance standards in developed countries like the United States include the National Institute of Standards and Technology (NIST) Cybersecurity Framework, Cybersecurity Information Sharing Act (CISA), and State Data Breach Notification Laws. The existing regulatory and compliance standards in South Africa include POPIA, CIIP and ECTA (Srinivas, Das and Kumar, 2019).

South African government and regulatory authorities recognise the significance of cybersecurity and have endorsed data protection laws and regulations specific to the energy and retail sectors. These laws include data security, consent, customer data protection, direct marketing, employee data protection and data breach notification that align with IT security policies with global cybersecurity standards such as ISO/IEC 27001, National Institute of Standards and Technology (NIST) cybersecurity framework, or industry-specific guidelines will ensure that the petroleum retail sector adopts best practices in protecting against cyber threats (Culot et al., 2021).

SA has its own data protection legislation known as the Protection of Personal Information Act (POPIA), which aims to aims to regulate the processing of personal information and ensure that individuals' privacy rights are protected (Staunton et al., 2021). Although this is the case, Warikandwa (2021) argues that South African organizations with international operations or dealing with the personal information of

European Union's (EU) citizens may need to consider General Data Protection Regulation (GDPR) compliance.

(Raul, 2019) states that the EU General Data Protection Regulation (GDPR) governs the collection and processing of personal data in all sectors of the European economy. According to Magalhães et al. (2023), GDPR provides data protection regulation for the entire EU, including various obligations on organisations that process personal information of individuals (data subjects) as well as giving data subjects rights related to processing of their personal information. Additionally, not adhering to GDPR regulations may be considered a criminal offense, carry heavy fines, and give result in legal lawsuits from harmed data subjects (Hoofnagle, Sloot & Borgesius, 2019).

POPIA shares similarities with the General Data Protection Regulation (GDPR) of the European Union in that it aims to protect the personal information of individuals and regulate how organizations handle such data. While POPIA is not identical to GDPR, it aligns with many of its principles and requirements such as data processing principles, consent, data subject rights, data breach notification, accountability and compliance as well as cross-border data transfers (Raul, 2019).

### 1.3.5 Employee training and cybersecurity culture

Capacity development, creating awareness and knowledge sharing are critical to promoting a cybersecurity culture among employees. While robust IT security policies are essential, they can only be effective if employees are educated and aware of cybersecurity best practices. Farheen Ansari (2022) states that employee training programs are crucial to inspire a security-conscious culture, empowering staff to identify and report potential threats promptly. Training instructions and guidelines, as noted by Viegas and Kuyucu (2022), are communicated to users through internal organisational communication and training channels or face-to-face training programs.

Studies have shown that cybersecurity challenges due to the introduction of 4IR persist and are often dominated by insider threats. Although organisations are known to possess robust and sophisticated IT security policies as a protective measure against cyberattacks (Danet, 2020), the insider threat posed by individuals who have privileged access to an organisation's resources, namely staff, contractors, and trusted third parties Rice and Searle (2022) has become a critical challenge. According to (Saxena et al.,

2020) IT-related incidents have increased in 2020 and global average cost of insider threats has risen by 31% to $11.45 million as employees are responsible for approximately 27% of data breaches, with phishing (67%) being the most common form of unintentional insider risk. These stats show that insiders do not realise the significance of security breaches as they unintentionally expose the organisations to outsider attacks (Khan, J. Houghton & Sharples, 2022). Based on the existing literature, it is clear that there are challenges associated with IT security policy compliance and adoption. According to Agrafiotis et al. (2018) employees are responsible for 27% of data breaches, with phishing (67%) being the most common form of unintentional insider risk. This demonstrates that certain employees in various organisations who do not adhere to IT security policies can potentially have a negative impact on IT security strategy and, after that, lead to business disruption, reputational damage, sanctions for non-compliance, and loss of business.

In light of the establishment of IT security policies and other interventions, insider threats remain a problem, and this study proposes an awareness model focusing on the use of IT security policies in the South African petroleum retail sector. The model aims to empower organisations to strengthen their cybersecurity defences, protect their digital assets, and ensure a secure and uninterrupted provision of essential services.

## 1.4 Significance of the Research Study

Based on the preliminary literature review, it is evident that IT security policy compliance poses challenges. It has been demonstrated that certain employees in various organisations do not adhere to IT security policies. As a result of these factors, IT security strategies may be negatively impacted. Ultimately, this can result in disruptions to business operations, reputational damage, and sanctions for non-compliance. The significance of this research study lies in its focus on addressing policy usage and compliance in the petroleum retail sector to enhance cybersecurity effectiveness. While there have been prior efforts in developing cybersecurity awareness models and frameworks, little attention has been given to the crucial aspect of policy usage and compliance in making these policies more effective.

This study acknowledges that IT security policy compliance poses challenges in various organisations. Identifying the factors that hinder compliance can help devise targeted strategies to overcome these barriers. By understanding the challenges that lead to non-

compliance, organisations can develop tailored solutions to promote policy usage and improve policy adherence and overall cybersecurity, including safeguarding sensitive information and protecting the organisation against insider threats. Ultimately, improved IT security policy compliance can lead to tangible benefits for the petroleum retail sector, such as preventing disruptions to business operations, preserving the sector's reputation, and mitigating the risk of penalties or sanctions for non-compliance with cybersecurity regulations.

This study employed an empirical case to provide insights into insider-related security breaches caused by a variety of factors such as human error, a lack of access control, and inadequate security controls. Organizations must invest in security strategies which incorporate both technical and non-technical measures to detect and safeguarding sensitive information from insider threats.

This research study provides an awareness model for using information technology security policies in the petroleum retail sector. This research is important as it can provide the petroleum retail sector with valuable knowledge and resources to effectively tackle cybersecurity concerns, improve policy compliance, and establish a secure, resilient, and full potential for IT security policy compliance.

## 1.5 Problem Statement

Stergiopoulos, Gritzalis & Limnaios (2020) argued that technology trends directly affect the petroleum industry since it distributes products requiring IT systems for manufacturing and distribution. As a result, IT security measures and processes need to be implemented to protect the industry and its customers from cyber-attacks, data breaches, and other malicious activities. According to Hamilton and Rauch (2022), The digital transformation of the oil and gas sector presents potential vulnerable opportunities for hackers, criminals, insiders to exploit and this contributes to the need for strong security measures.

Cybersecurity issues result from insider threats, even in organisations with well-developed IT security policies and sophisticated technology to protect against cyberattacks. Mittal and Garg (2022) claims that between 60 and 70 percent of attacks on organizations are carried out by insider employees, suggesting that insiders have the ability to expose organizations to outside attacks without understanding the significance

of security breaches. According to (Homoliak et al., (2019), insiders may not comply with security policies that are in place and may not understand the implications of their actions, allowing them to expose the organisation to risks without intention. Furthermore, Alsowail & Al-Shehari (2020) argued that, because insiders have preferential access to an organization's most sensitive assets, insider threats are more challenging to prevent than external ones. Several research have examined insider threat detection techniques from both theoretical and taxonomical positions. However, empirical defense technologies are needed to prevent insider threat challenges.

This study focuses on an awareness model for the use of Information Technology security (IT security) policies in the petroleum retail sector.

## 1.6 Research Questions

In order to better address the research problem, the research questions have been framed in terms of the Technology-Organization-Environment (TOE) framework developed by Depietro et al. (1990).

TOE considers three factors influencing adoption decisions: technology, organisation, and environment. Technology includes the capabilities of the technology, its usability, and the resources necessary to implement and use it. Organisation includes management support, user education, and user experience. Environment refers to external factors, such as market conditions, competitor offerings, and legal/regulatory requirements (Chandra et al., 2018).

This study presents one main research question (MRQ) and three supporting questions.

***MRQ: How can an awareness model be developed to improve the use of IT security policies in the petroleum retail sector?***

The sub-questions (SQ) necessary to support the main research question are listed below:

***SQ1: What IT security controls or policies are in place to protect organisational information?***

***SQ2: What organisational factors are used to promote IT security policy compliance and adoption?***

***SQ3: What challenges are experienced with IT security compliance in the organisation?***

## 1.7 Research Objectives

The main objective of this study is to develop an awareness model for the use of IT security policies in the petroleum retail sector. In order to accomplish this, one main research objective (MRO) and three supporting objectives have been formulated.

***MRO: To develop an awareness model for the use of Information Technology security (IT security) policies in the petroleum retail sector.***

The sub-objectives (SO) necessary to support the main research objective are listed below:

***SO1: To determine IT security policies and controls that are in place to protect organisational information.***

***SO2: To explore organisational factors used to promote IT security policy compliance***

***SO3: To discover challenges experienced with IT security policies in the organisation***

## 1.8 Delineation of the research

The scope of the study is described in the section titled **Error! Reference source not found.** and the population is described in Section 4.9 titled Sampling/justification. Thus, the focus is only limited to the petroleum retail sectors in Cape Town.

The researcher may have difficulty gaining access to the petroleum retail sectors, and participants may not be interested in participating. As an employee of a petroleum retail company and having observed the empirical case of this study, the researcher has chosen this sector and can explain to management how important this research is to their operations.

## 1.9 Structure of thesis

The structure of this thesis is outlined as follows:

- **Chapter One** presents the background to the research and the research problem. The research objectives and significance of the research study are also clearly described. Chapter two of this research focuses on the literature review relevant to this study and provides background to the imperial case and cybersecurity.
- **Chapter Two** of this research study focuses on the literature review relevant to this research. This chapter provides insights into previous and existing research on the topic. It also provides insights into the theories, models, and concepts relevant to this research. This study is built on an understanding of the imperial case and cybersecurity.
- **Chapter Three** explores the theoretical frameworks and conducts a comprehensive investigation and analysis of the five theoretical frameworks related to this study. It explains their effectiveness and discusses the strengths and weaknesses of each framework in guiding the research study.
- **Chapter 4** provides a detailed explanation of the research design and methodology used in this study, including a discussion of the specific research strategy and approach adopted. This chapter additionally presents a detailed description of the study tools and methods and clarifies the data collection process. In addition, the chapter explores the ethical considerations related to this study.
- **Chapter 5** provides the study's findings and a comparative analysis of the data collected and the study's results. It also compares the results to the predictions made at the beginning of the study and discusses the implications of the findings.
- **Chapter 6** presents the discussion, conclusions, contributions, limitations, and recommendations of this study.

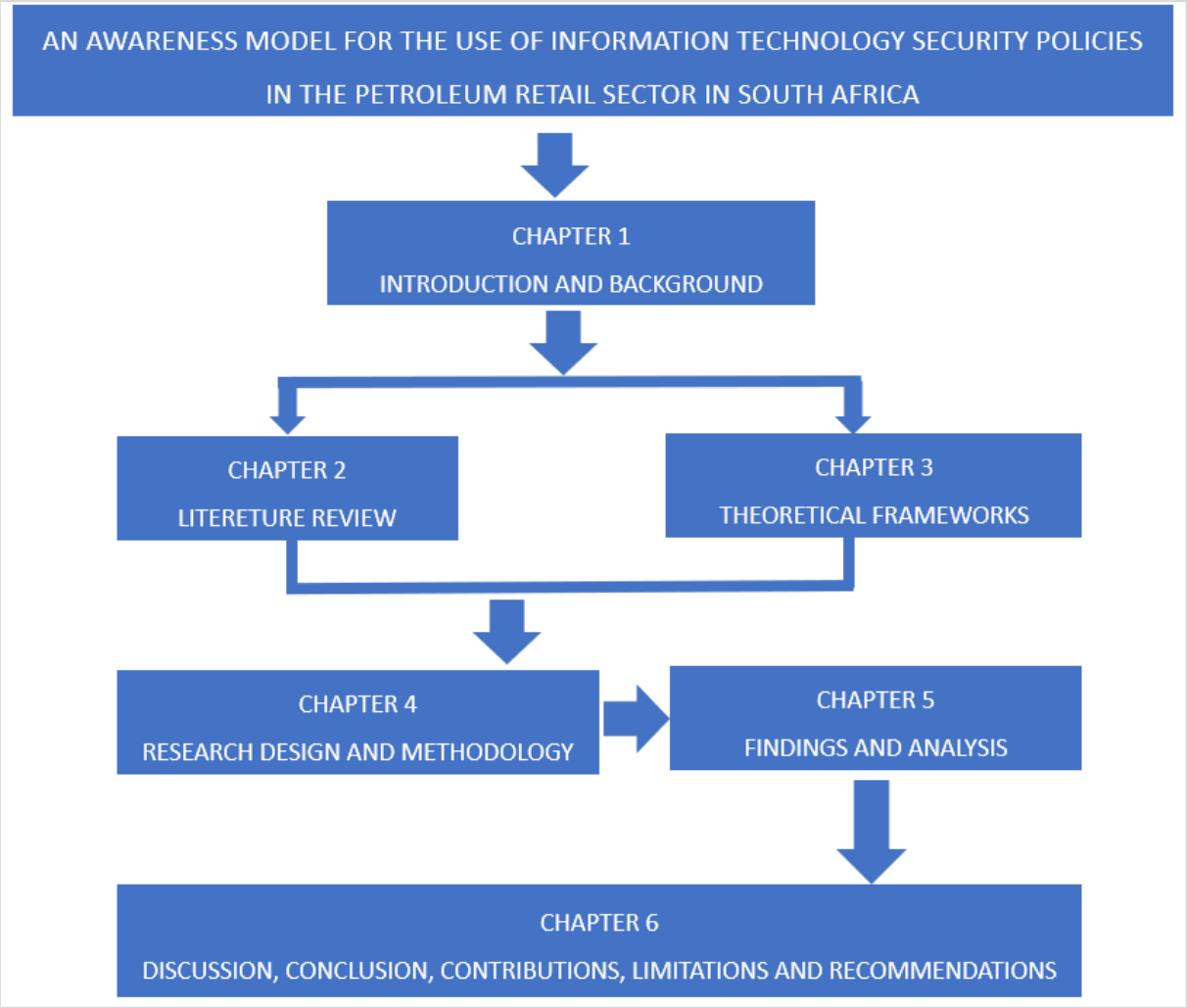



*Figure 1.1 Thesis Structure*

## 1.10 Chapter Summary

The introduction highlights the importance of information technology security policies in the petroleum retail sector in South Africa. It emphasises the sector's digital transformation and adoption of advanced technologies, which have improved operational efficiency and competitiveness. However, it also acknowledges the need to address cybersecurity challenges to protect against potential threats. The introduction sets the context for the research and the significance of developing an awareness model for the effective use of IT security policies in the sector.

The background section provides additional context for the research study, emphasising the significance of cybersecurity incidents in the process industry. It explains how cyber incidents can lead to economic and reputational damages and major accidents with severe consequences for workers, the population, and the environment. Recognising the importance of information security policies, the section mentions the efforts made by the South African government and regulatory authorities in enacting data protection laws specific to the energy and retail sectors. Additionally, it emphasises the need for aligning IT security policies with global cybersecurity standards to ensure best practices in protecting against cyber threats.

# CHAPTER 2
# LITERATURE REVIEW

## 2.1 Introduction

This chapter provides an empirical case study and conducts a thorough review of pertinent literature related to the study's topic. The literature review is conducted to enhance comprehension of existing research and the theories that underpin this study. This, in turn, facilitates a more extensive analysis and the formulation of a comprehensive research model.

## 2.2 Empirical case

The empirical case provides additional information about a specific petroleum retail sector.

The organisation is a petroleum retail company in South Africa (SA) with 700 retail sites in all SA provinces and six neighbouring African countries.

The organisation:

- Consists of personnel from divisions such as IT, finance, HR, retail, legal, and supply chain.
- Experienced security breaches related to insider threats caused by employees and third-party vendors (compromised credentials and unsecured links)

The security breach resulted in the organisation experiencing business disruptions because the compromised system was isolated, and there was no redundancy system during the downtime. The system was unavailable for several days until a new server was built, patched, and configured. The issue resulted in financial loss related to project delays, and further risks could have been experienced if data was leaked, such as additional financial loss, loss of stakeholder and system trust, and IT reputation to the business.

The following issues related to the incident were identified:

1. **Personnel:** Issue of adherence to IT security policies. The petroleum retail company has already established IT security policies, but some personnel fail to follow them. Organisational culture is an issue when putting what has been learned into practice.
2. **Technology:** Single sign-on (SSO) not implemented on work applications; personnel have to remember multiple complex passwords, and as a result, in order to remember, passwords are usually saved on applications such as Excel and Notepad
3. **Environment:** Security and cyber training does not cater for external third-party vendors; the focus is usually on permanent staff

Although policies and training programmes exist to promote cybersecurity awareness, the petroleum retail sector lacks a model to encourage compliance and adoption of IT security policies. As a result, insider-related security breaches continue to occur.

## 2.3 Cybersecurity

This chapter provides a comprehensive understanding of the potential threats to cybersecurity, such as data breaches, phishing attacks, and malware, as well as strategies and tools to mitigate these threats.

The Internet of Things (IoT) and digitalisation are becoming increasingly important for several reasons. In recent years, there has been an increase in cybersecurity-related concerns such as unauthorised access, malware attacks, and zero-day attacks. For instance, data breaches have become a frequent occurrence in addition to denial of service (DoS) attacks, social engineering attacks, and spear phishing attacks (Sarker et al., 2020).

Therefore, organisations must adopt a robust cybersecurity mitigation step to ensure that their networks are protected and have policies and procedures in place to protect their data and systems. Dash & Ansari (2022) describe that the awareness of risks associated with cybersecurity is critical for the organisation. It details the extent to which the company is prepared for any type of cyber attack and evaluates the employees' level of

familiarity with the subject matter. Furthermore, Ali et al. (2021) highlight that, for an organisation to claim that they have awareness throughout their ranks, the employees and the organisation ultimately need to be exposed to the threats while receiving additional instruction on the causes and effects of each threat alongside how to prevent and combat the threat. In this way, the managers and security specialists of the information system will not have to deal with the majority of the dangers to the company's information security because the employees will feel more responsible.

### 2.3.1 Internet of Things (IoT) devices

The growing number of Internet of Things (IoT) devices has experienced a significant rise in recent years. As of 2020, the global usage of Internet of Things (IoT) devices was forecast to range between 10 and 15 billion and is expected to exceed $1.5 trillion by 2030 (Al-Sarawi et al., 2020). Projections suggest that this number is expected to experience substantial growth in the future.

- **Sensor Deployment**: IoT sensors are widely used in oil and gas operations to collect real-time data on temperature, pressure, flow rates, and equipment health (Honeycutt et al., 2021).
- **Predictive Maintenance**: IoT-enabled predictive maintenance helps reduce downtime and optimise the lifespan of critical equipment, such as pumps, compressors, and pipelines (Robatto Simard, Gamache & Doyon-Poulin, 2023).

IoT presents a wide range of challenges when it comes to cybersecurity. As more and more devices become connected, the potential for data breaches and cyber-attacks increases. The following key challenges are frequently linked to cybersecurity in IoT devices:

- **Insecure Communication:** Internet of Things (IoT) devices frequently utilise networks and vulnerable communication channels that might be manipulated by malicious actors. Poor encryption, the absence of secure authentication routes, such as VPN-based authentication, as well as inadequate data integrity protection can result in the exposure of sensitive information to unauthorised intruders (Masuduzzaman et al., 2019).

- **Privacy Concerns:** Internet of Things (IoT) devices frequently gather and transmit substantial personal data. Privacy concerns occur when this data is inadequately protected. Unauthorised access to personal data might result in identity theft or unlawful spying (Onu, Kwakye & Barker, 2020).
- **Firmware and Software Vulnerabilities:** A significant number of Internet of Things (IoT) devices operate on embedded systems that often lack frequent firmware updates. If security patches are not promptly applied, attackers can exploit vulnerabilities in firmware or software (Wijesundara et al., 2023).
- **Lack of Standardisation:** The lack of defined security standards and procedures in the IoT industry can result in inconsistencies in implementing security measures. The absence of consistency makes it challenging to set a baseline and standard for security measures (Tawalbeh et al., 2020).

An integrated approach that incorporates technological innovation solutions, policy and compliance frameworks, and collaboration among stakeholders is necessary to establish a more secure Internet of Things (IoT) environment. A robust cybersecurity plan for the Internet of Things should include ongoing monitoring, sharing threat intelligence, and the implementation of security protocols at every stage of the IoT device's lifecycle.

### 2.3.2 Artificial Intelligence

Undoubtedly, artificial intelligence (AI) significantly affects cybersecurity by improving defensive measures and shaping the strategies employed by cyber attackers. According to Rizvi (2023),AI systems can quickly identify and react to possible dangers, while malicious individuals are increasingly using AI approaches to avoid being detected and to generate synthetic media, which can be utilised for the purpose of disseminating misinformation or initiating phishing attacks (Bazarkina & Pashentsev, 2020).

Artificial intelligence (AI) substantially enhances cybersecurity across multiple critical domains, such as:

- **Phishing Detection:** Artificial intelligence can be utilised to identify and prevent phishing attacks by analysing e-mail patterns and detecting elements that appear suspicious. Natural language processing (NLP) algorithms have

the capability to analyse the content of e-mails in order to detect indications of phishing attempts (Salloum et al., 2022).

- **Vulnerability Management:** AI can aid in the identification and prioritisation of vulnerabilities in systems such as endpoint devices (computers and mobile devices), servers, and applications by analysing data on established vulnerabilities and prospective paths for exploitation. This allows security teams to concentrate on resolving the most crucial system weaknesses (Yildirim, 2021).
- **Enhanced Authentication:** AI contributes to the improvement of authentication mechanisms. Biometric authentication, facial recognition, and behavioural biometrics are examples of AI-powered technologies that enhance the security of access controls to help reduce the risk of unauthorised access to systems and data (Raghavendra, Omprakash & Kamath, 2021).
- **Behavioural Analysis:** Artificial intelligence facilitates the development of behavioural analysis tools that acquire knowledge and understanding of the typical behaviour performed by people and systems. Any deviation from these acquired patterns can be identified as potentially harmful behaviour, enhancing the capability to detect insider and advanced persistent threats (Mehra and Badotra, 2021).

Although AI provides significant benefits to cybersecurity, it also introduces new challenges. Bazarkina and Pashentsev (2020) state that AI systems can be exposed to adversarial attacks, whereby malicious actors can manipulate them to get desired results. Moreover, it is essential to evaluate and consider the ethical implications of leveraging AI in cybersecurity, including the possibility of violating privacy.

### 2.3.3 Cloud-Based Systems

Using cloud computing technology in the petroleum industry has become an increasingly popular way to provide flexibility when it comes to computing power and storage capacity, which reduces the complexity and control time necessary in the production process (Vladimir Yu. Turchaninov et al., 2018). According to Zhifeng (2019), cloud technology can also be used to automate processes, which is especially useful in the oil

and gas industry, where processes are often complex and require large amounts of data to be processed.

In the evolving landscape of the petroleum industry, the following key technological advancements are making a substantial impact:

- **Cloud Services:** Many companies in the petroleum sector have transitioned their data storage and processing to cloud-based systems, enabling scalability and remote access (Gundu, Panem & Thimmapuram, 2020).
- **Data Analytics:** Cloud-based analytics platforms are used for processing and analysing vast volumes of data generated by IoT sensors, allowing for insights into production optimisation and cost reduction (Saleem & Chishti, 2019).
- **Tank Simulation:** In the oil and gas industry, cloud-based simulation tools have been developed to optimise tank performance. These tools enable petroleum engineers to model and simulate tank behaviour, resulting in more efficient oil and gas recovery. Simulations can provide insight into the performance of tanks, enabling engineers to make informed decisions and optimise tank operations. This can increase oil and gas industry efficiency, decrease costs, and increase output (Hussain et al., 2022).
- **Supply Chain Management:** Cloud-based solutions in supply chain management have become increasingly prevalent and are transforming how businesses plan, execute, and optimise their supply chain operations. These solutions leverage cloud computing technology to provide a range of benefits, including improved visibility, scalability, collaboration, and efficiency (Alam, 2021).

Cloud-based systems also offer unique challenges in the field of cybersecurity. Addressing these challenges is critical for organisations to protect the security and privacy of data in cloud settings. The following are some key challenges presented by cloud-based systems in cybersecurity:

- **Identity and Access Management (IAM):** Managing user identities and regulating access to resources in a cloud environment might provide difficulties. Organisations must establish efficient IAM policies to prevent unauthorised access and guarantee relevant authentication and authorisation (Wang, Chen, 2020).

- **Data Loss and Leakage:** Accidental data loss or leakage is a concern in cloud environments. Misconfigurations, inadequate access controls, or insider threats can lead to data exposure (Komal, 2023). According to (Hassan et al., 2020), the implementation of data loss prevention (DLP) measures and monitoring for unusual data access patterns are crucial.
- **Insecure Interfaces and APIs:** Cloud environments rely heavily on interfaces and APIs for interaction. Insecure interfaces and APIs can be exploited by attackers to compromise data and systems (Genfer & Zdun, 2022). Regularly assessing and securing these entry points is critical.
- **Limited Visibility and Control:** Organisations may have limited visibility into their cloud providers' infrastructure and security controls (Rizvi, Bolish & Pfeffer, 2017). This lack of control can be a challenge for organisations aiming to enforce specific security policies and practices.

### 2.3.4 Interconnected Networks

Interconnected networks play a crucial role in the petroleum industry, allowing for efficient operations, data administration, and safety measures throughout the value chain. Within the complex infrastructure of the industry, these networks facilitate communication, data transmission, and control. Here are key examples of interconnected networks in the petroleum industry(Xie, Wei & Zhou, 2020):

- **Communication Networks:** Robust communication networks are essential for the petroleum industry. Oil and gas companies invest in private networks and satellite communications for remote and offshore locations (Wanasinghe et al., 2020).
- **Industrial Control Systems (ICS):** Many oil and gas facilities employ interconnected monitoring and controlling critical processes, focusing on safety and reliability (Moradbeikie et al., 2020).
- **Smart Oilfields:** Interconnected networks are used in the development of smart oilfields, which integrate real-time data from various sources to optimise drilling, production, and reservoir management (Moradbeikie et al., 2020).
- **Pipeline Monitoring:** IoT sensors and interconnected networks are used to monitor pipeline integrity, detect leaks, and ensure the safe transportation of petroleum products (Joshi, Munjal & Karanje, 2019).

The presence of interconnected networks, particularly within the realm of the Internet and complex infrastructures, presents various challenges in the field of cybersecurity. According to Sarhan (2023), cyber-attacks pose a greater threat to interconnected networks due to the ability of attackers to target several systems simultaneously. Moreover, interconnected networks necessitate supplementary security protocols to safeguard data from unauthorised intrusion and managing interconnected networks can provide greater challenges as they necessitate sharing and monitoring data across many platforms (Ragab & Altalbe, 2022).

### 2.3.5 Social engineering attacks

According to Salahdine & Kaabouch (2019) Social engineering (SE), also known as human hacking in cybersecurity, refers to the practice of acquiring information through technical and non-technical methods. Furthermore, Steinmetz (2022) states that SE is a tool used by unauthorised personnel to gain access to sensitive information. This includes gathering information from public records, searching the Internet, and using illegal or fraudulent techniques such as phishing e-mails or impersonating others on the Internet to obtain this information (Aldawood & Skinner, 2019). Social engineering is widely regarded as a serious threat to infrastructure, data, and cyberspace operations (Radhika, Mathur & Nanda, 2022).

Despite the evolution of social engineering techniques over time, the success of a social engineering attack still depends on modern preventative tools, security systems, and the availability of trained and skilled personnel (Aldawood & Skinner, 2019).

According Wang, Sun and Zhu (2020), the cost implication and frequency of cybersecurity threats on corporate organisations indicated that social engineering was the top cyber threat to organisations. Additionally, Wang, Sun and Zhu (2020) states that social engineering attacks affected 85% of organisations in 2018, an increase of 16% from 2017.

In 2018, social engineering attacks cost organisations an average of $1.4 million, an increase of 8% from 2017 (Alsulami et al., 2021). In developed countries such as the United States, the United Kingdom, Canada, Australia, New Zealand, and Germany,

social engineering attacks were approximately 48% of large companies, and 32% of companies of all sizes experienced an average of 25 SE-related threats (Liu et al., 2023).

Figure 2.1 below shows three levels of social engineering attacks: the physical level, the technical level, and the psychological level:

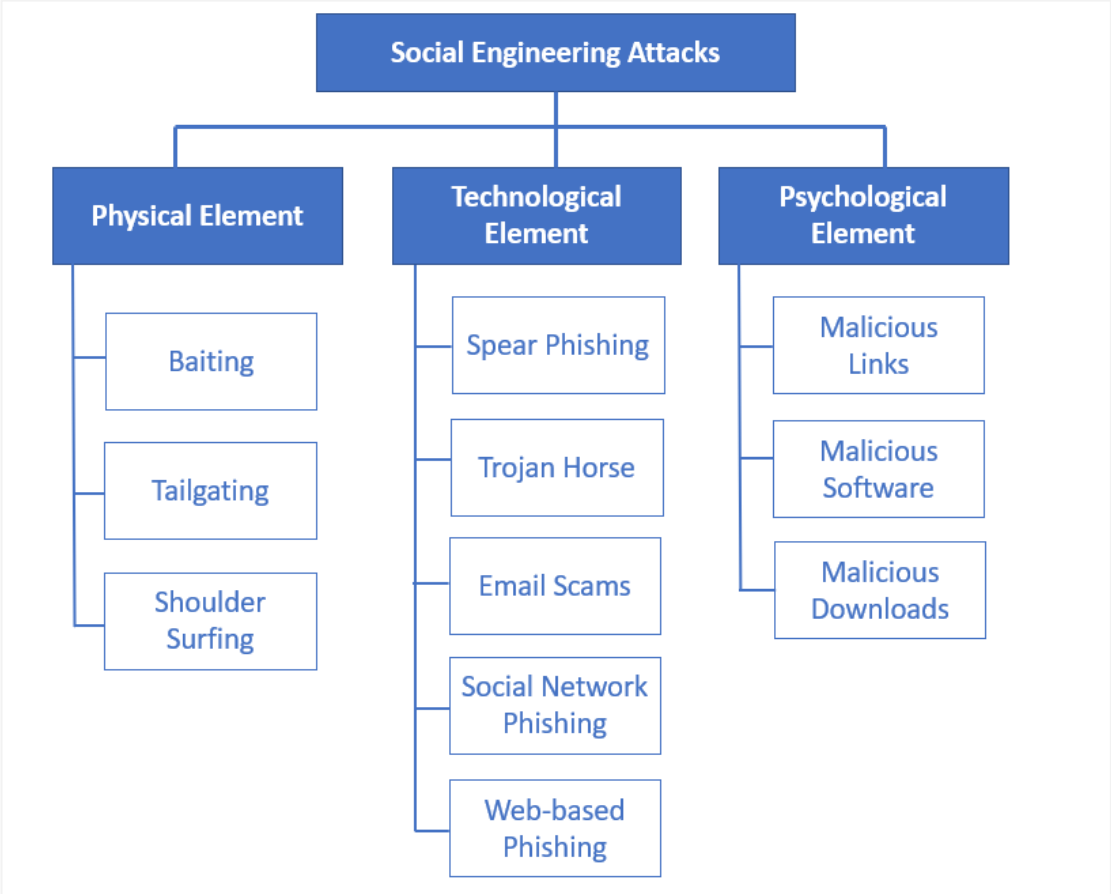



*Figure 2.1 Social Engineering Attacks Elements*

Source: Adapted from Wang, Sun & Zhu (2020)

#### 2.3.5.1 The physical element of social engineering

Research conducted by Salahdine and Kaabouch (2019) defines "physical-based attacks" as those in which the attacker makes physical contact with the target in order to get access to sensitive data. Physical entry, shoulder surfing, dumpster diving, phone

social engineering, pretexting, impersonating on support desk calls, and theft are all examples of these types of attacks.

At the physical level, cyber attackers use physical force to gain unauthorised access. In cybersecurity, physical attacks involve stealing documentation and hardware (e.g., laptops, servers), tampering with equipment, physically disrupting communication lines, shoulder surfing and tailgating to gain access to a secured system or environment. The consequence of the physical element of SE is data loss within the organisation (Salahdine & Kaabouch, 2019)

Physical attacks can be carried out by outsiders or insiders (Wang, Sun & Zhu, 2020):

- **Outsiders** can gain access to the premises by using force or exploiting weaknesses in the physical security system, such as posing as maintenance workers or consultants and then taking over the office. The attacker might find passwords lying around or watch an oblivious employee key in the password through shoulder surfing.
- **Insiders** can use their access to the premises or building to cause damage to equipment and data or even physically remove hardware or data from the premises.

#### 2.3.5.2 The technical element of social engineering

In the technical element of social engineering, attackers use sophisticated technology through computers and mobile phones to access sensitive information, resources, or confidential documents through user's passwords. The technical element of SE involves using malicious actions to request the download of malware (Rodriguez, Atyabi & Shouhuai, 2022). The successful technical element of SE is in the use of human behaviour to predict and identify the weakest link in any security system. It is, therefore, critical for organisations to be aware of attacker methods and take steps to protect themselves. Taking measures such as using strong passwords, incident response plans and educating employees on security policies and behaviour can protect the organisation against social engineering attacks and breaches.

Wang, Sun & Zhu (2020) argued that Spear Phishing and Trojan Horse are excellent examples of technical attacks, and attackers have used them to gain access to sensitive data. Aldawood and Skinner (2019) describe Spear Phishing as a form of attack that is usually referred to as an Advanced Persistent Threat (APT). The APT is used to access a system of information and is commonly used to commit financial fraud. This kind of attack typically targets a certain set of employees in a business entity. Employees' e-mails, social profiles, websites, and blogs are attacked by sending fraudulent e-mails or links that appear legitimate to trick someone into providing confidential information. The Trojan Horse is a malicious software program often disguised as harmless or legitimate programs used to steal confidential information or gain access to a user's system.

Non-compliance behaviours related to sharing corporate data via social media are a worldwide problem. Social media platforms have become a significant risk for corporations since employee activity can jeopardise critical company information (Shen, 2023). The information security threats related to social media use are complex and require information professionals to participate in ongoing security training (Kshetri, 2013). According to Zamir (2020), neglecting to resolve these security concerns can significantly affect an organisation's reputation, loss of customer trust, and financial losses. As such, a comprehensive framework is needed to address the complexities of privacy and security issues associated with social media while considering the multifaceted influences of institutions and technology.

#### 2.3.5.3 The psychological element of social engineering

At the psychological level, Wang, Sun & Zhu (2020) describes that attackers use psychological techniques and manipulative tactics to gain access to confidential data. This includes social engineering techniques such as impersonation, deception, influence, and manipulation to gain access to confidential information. For instance, attackers can also use phishing tactics to get users to click on malicious links or download malicious software in an attempt to acquire sensitive information.

Information security professionals face a challenging situation when dealing with a social engineering attack since no technological countermeasure has yet been found to potentially eliminate human vulnerabilities. Social psychology studies demonstrate that

alternative routes to persuasion, attitudes, and beliefs that affect human interaction, as well as techniques for persuasion and influence, provide psychological vulnerabilities for social engineering attacks (Conteh & Schmick, 2016). According to Aldawood and Skinner (2019), attackers use e-mail scams to attack victims. This includes the use of hyperlinks to confirm banking details, e-mail letters to offer jobs, and notices from SARS (South African Revenue Services) to establish contact. E-mails are created to appear as though they are coming from reliable sources, making organisations vulnerable to such attacks. This spoofing pattern indicates that social engineering attacks are aligned with businesses' efforts to implement protective measures. In the case of social engineering, the weakest link in the chain of computer security is exploited, and the attacker targets the human aspect of security, taking advantage of the natural tendency to trust and use psychological manipulation to obtain confidential information or access to restricted systems (Salahdine & Kaabouch, 2019).

### 2.3.6 Operating system hardening and configurations

According to Satrya, Cahyani and Andreta (2015), malware authors target a Microsoft windows operating system more often than other operating systems because it is the most common OS. Microsoft also releases security updates more frequently than other operating systems, making it easier for intruders to introduce vulnerabilities.

Hamdani et al. (2021) illustrates that operating system (OS) hardening is an essential component of cybersecurity which includes various measures to improve the security posture of an operating system and the overall network infrastructure.

Operating system (OS) configuration influences the system's security posture thereby affecting its reliability. Configuring operating systems securely to mitigate potential vulnerabilities and prevent cyber threats presents a number of challenges and gaps (Dissanayake et al., 2020):

#### 2.3.6.1 Default Configurations

Many operating systems offer default configurations that prioritize ease of use over security. For example, some operating systems may not require strong passwords to login, might contain open ports and lack encryption. Thus, the system may be vulnerable to attacks. Security administrators must examine and modify the default settings to make sure a more secure environment is established (Stanek, 2017).

#### 2.3.6.2 Access Control and User Permissions

It might be challenging to manage user permissions and access management. It is important to ensure that users have the essential permissions without providing them excessive privileges. Misconfigurations can allow unauthorized access and result in security breaches (Meier, Fuchs & Pernul, 2013).

#### 2.3.6.3 Patch Management

Updating the operating system with the latest security patches is crucial. However, managing patch deployment across a large number of systems, testing for compatibility, and ensuring minimal disruption to operations can be challenging Dissanayake et al. (2020). Without proper patch management, organisations may be exposed to cyber threats or be forced to deal with unexpected downtime

#### 2.3.6.4 Network Configuration:

Firewalls, data encryption, intrusion detection/prevention systems, and ensuring secure communication channels can be complex to configure, especially in large and dynamic networks. To maintain good security posture, network configuration must be properly established and regular assessments on the configuration of the network must be conducted so that necessary steps can be taken to eliminate any security gaps and or vulnerabilities (Aslan et al., 2023).

#### 2.3.6.5 Endpoint Security Configuration:

According to (Arfeen et al., 2021)The configuration of security features on endpoints, such as antivirus software, endpoint detection and response (EDR) tools requires careful consideration to eliminate conflicts and ensure comprehensive protection. Furthermore, it is important to regularly update endpoint security tools to ensure they are effective against the latest threats.

Zheng et al. (2022) assert that it is important for organisations to stay updated with the latest patches and other security measures such as enabling firewalls, installing antivirus software and implementing security policies such as requiring stronger passwords, multifactor authentication (including number matching) as they all contribute to a secure operating system's security posture. Dissanayake et al. (2020) emphasises that

organisational policies and the network administrator's skills are crucial to influence the complexity of vulnerability management. However, human and technology interactions always exist, and human error is always likely to happen, regardless of how secure an operating system is. For example, if an employee clicks on an unsafe link or installs a software with a virus, that virus can gain access and take over the entire operating system.

Shukla et al. (2022) states that predefined security standards, such as NIST, Common Criteria (CC), and ISO, can be used to maintain and optimize systems as required. Network security administrators can manually follow these security standards to strengthen the operating system security, and there may be an automated system that tests the entire integrity of the system and generates a report to measure compliance depending on existing configurations. Klein and Zwilling (2023) further state that companies can implement regular employee training to ensure that employees are up to date on the latest security threats. Additionally, companies can invest in security software that can detect and block operating system threats before they can cause any damage.

#### 2.3.6.6 Password and MFA Setup

An organisation's security can be enhanced by implementing strong passwords and a Multi-Factor Authentication (MFA) process. MFA provides an extra layer of security by requiring two or more credentials, such as a password and an authenticator approval request sent to your mobile phone. This is to gain access to an account and making it difficult for attackers to gain access to an account (Meyer et al., 2023). Although these safety measures are critically important, they do not guarantee that accounts will be secure. Haro (2017) state that, hackers are always coming up with new methods to access accounts and data, so even the strongest policies can be compromised. Organisations must maintain vigilance and update security measures on a regular basis.

**Implementing the Strong Password Process**

According to Kävrestad et al. (2019), establishing and enforcing passwords that are at least 12 characters in length using uppercase and lowercase letters, numbers, and special characters ensures that the user's password is secure and difficult to breach. The longer the password, the harder it is for hackers to guess, as there are more possible

combinations. Additionally, the combination of uppercase and lowercase letters, numbers, and special characters makes it harder for hackers to crack the password using automated tools.

A study by Yildirim and Mackie (2019) indicate that despite the implementation of strict password policies, users adopt copy paste mechanism such as writing passwords down or saving them in documents like excel, notepad, and word. To support complex passwords, password guidelines and awareness must be in place and enforced.

According to Jalali, Assadi and Osman (2023), most individuals struggle with managing multiple passwords for various accounts. Remembering numerous difficult passwords can lead to stress, confusion, and worry. Jalali, Assadi and Osman (2023) further argues that, to avoid these negative consequences, individuals may choose easily accessible passwords like "123456" or "password" or reuse the same password for multiple accounts. This is a risky practice since if one account is compromised, all accounts with the same password are vulnerable. Systems should be configured to prevent easily guessable and repeat passwords. Gautam and Singh (2022) state that, hackers use automated programs to guess passwords based on common patterns, allowing them to obtain access to organisational data and information.

**Implementing the Multifactor Authentication (MFA) process**

Multi-factor authentication (MFA) is an increasingly popular security mechanism used in internet-based applications to validate the identity of the user attempting to access the content. MFA is an authentication method that adds to a regular username and password by requiring the user to provide some additional authentication code or information that only they have (Williamson & Curran, 2021).

According to Meyer et al. (2023), implementing MFA including number matching for critical applications such as email, virtual private network (VPN), and SharePoint provides an extra layer of protection, lowering the probability of compromise by 99.22% across the population and 98.56% in instances where there are leaked credentials. As a result, multi-factor authentication (MFA) can improve organizational security.

An additional layer of security can be provided by the use of biometric authentication (fingerprints and face recognition) as part of the authentication process. This type of authentication is more secure and less likely to be compromised than other methods.

Furthermore, biometric authentication eliminates the need to remember passwords, making it more convenient for users (Basare, Bhojak & Solanki, 2023).

### 2.3.7 Safeguarding cybersecurity using control types

In order to safeguard against cybersecurity threats, Winfred et al. (2020) suggest different types of controls, including managerial, operational, and soft controls, are other names for administrative controls deployed to maintain cybersecurity. A control is a technique, procedure, or policy that has been developed and put into effect in response to threats and attack vectors that exist in a specific application software, system, or domain. It is a mechanism to protect unauthorised access to information and reduce the risk of cyberattacks. Security controls can be divided into three categories: technological, administrative, and tangible. They also comprise the tactics, processes, and strategies put in place to achieve security goals (Winfred et al., 2020). Maasberg et al. (2020) state that administrative controls involve the personnel factor of the organisation and include training and awareness programs, security policies and processes to control which users have access to which system and information in the organisation. Onumo, Ullah-Awan and Cullen (2021) assert that the ISO/IEC/TRl 13335-1 2004 standard suggests that personnel must share in the organisation's security vision, comprehend their roles and responsibilities, and develop practical implementation skills to secure and sustain cyberspace infrastructure and assets. Employees are trained to implement security controls, informed about the necessity of such controls, and made aware of their varied roles and duties throughout the organisation's security process. These controls are primarily designed to protect organisations against monetary losses caused by the actions of their employees. In addition, complementary controls such as rules, standards, procedures, and guidelines outline how different stakeholders should respond to cybersecurity problems.

### 2.3.8 Prevention, detection, and response against cybersecurity

Conteh and Schmick (2021) state that organisations are gradually enhancing their security systems to ensure that if one of the outer layers fails, one of the inner layers will prevent a threat from developing into a major crisis (multi-layer defence). A multi-layer defence structure includes the following precautionary measures to help protect sensitive data, and reduce the risk of a security breach and reputational damage related to human error:

- **Security policies and processes:** An effective security policy should include technical and non-technical approaches that the executive management team drives downward. Security must be integrated into every organisation's strategic and operational objectives and within its divisions and departments. This approach ensures that security is not an afterthought but an integral part of the organisation's operations and decision-making processes. It also ensures that there is a unified vision and strategy for security, which can be reinforced at all levels of the organisation (Tkachenko et al., 2019).
- **Identity and Access Management:** Access management is implemented by organisations to safeguard digital assets by reducing vulnerability to attacks and countering risks such as unauthorised access, data breaches, and insider threats. Access management includes establishing policies that govern the permissions for viewing, modifying, and deleting an organisation's digital assets. It also involves the implementation of security measures such as authentication, encryption, and firewalls. This measure ensures that the organisation's digital assets are accessible only to authorised individuals and that any possible intruders are prevented from gaining access to them (Devlekar & Ramteke, 2021). According to Shen (2023), improperly configured access controls can result in significant data leaks and system vulnerabilities, posing risks such as unauthorised access and data breaches.
- **Training and education programs:** In the early stages of employment, a new employee should attend a training session as part of the orientation process and subsequently attend refresher course training sessions. Users are exposed to social engineering tactics and behaviours commonly used by social engineers, thereby increasing awareness. Training and education programs help to create a culture of security within the organisation, and employees are better informed of the potential risks to which they may be exposed. They also teach employees how to identify and respond to suspicious behaviour to better protect themselves and their organisations from potential threats (Sas et al., 2021).
- **Audits and compliance checks:** It is essential for an organisation to engage in proactive monitoring of its security policies in order to ensure adherence to standards. Detective controls may be used to enhance security measures, encompassing the systematic examination of network logs, periodic re-

evaluation of employees' permissions, and regular inspection of desktop configurations. Through the active monitoring of compliance, an organisation can promptly detect any discrepancies or irregularities that may suggest a breach of security. Furthermore, it might be advantageous to ascertain if personnel are adhering to the security policies of the organisation, hence mitigating the likelihood of a breach transpiring in the first stages (Al-Matari et al., 2021).

- **The technical procedures:** Multiple layers of security must be implemented on a network to protect sensitive data and core infrastructure. Every device should be protected from intrusion by installing and configuring intrusion detection software (IDS), intrusion prevention software (IPS) and firewalls. Web filtering and VPN should be installed for all external facing demilitarised zones (DMZ). Having multiple layers of security makes it much harder for attackers to gain access to the network and any of the data stored on it. IDS, IPS, and firewalls can help detect and prevent unauthorised access. DMZs can help protect internal networks from outside threats. Web filtering can help protect against malicious website traffic, while VPNs can help ensure secure communication between remote users and the network (Georgi Tsochev et al., 2020).

Table 2.1 shows high-level technical IT security controls that organisations use to protect information.

*Table 2.1 IT security Controls*

| **High-Level Technical Controls** | |
|---|---|
| Control | Description |
| Unmanaged (MAM) and Managed (MDM) mobile devices | Where personal or corporate-owned mobile devices access corporate resources |
| Multifactor or Two-Factor Authentication (MFA/2FA) | Access to corporate resources using additional authentication in the form of a token, call or authenticator app |
| Transport Layer Security (TLS) or Internet Protocol Security (IPsec) | Access to the company's internet public websites is encrypted, and remote connections to internal services are encrypted |
| Centralised Endpoint Management | Centralised system for managing and administering distributed systems of computers running operating systems such as Windows, macOS and Linux. Provides patch management (quality and security), threat management, software distribution and network access |
| Antivirus | System that can scan, detect, prevent and delete malware from computer systems |
| Full Disk Encryption | Disks are encrypted on hardware to prevent unauthorised access to the data storage |

Source: Adapted from Viegas & Kuyucu (2022)

- **Physical Guidance:** Protecting physical assets can be achieved in a variety of ways. An effective way of deterring intruders from entering the premises is through the use of security guards, mantraps, and cameras (Reid, 2020). Organisations should ensure access is controlled whenever physical hardware is present. Simukali, Phiri and Namukolo (2019) state that this can be done using multifactor authentication, biometrics, or access control lists to maintain security. This ensures that only authorised personnel are allowed access to the premises and that any unauthorised access is immediately detected, and action can be taken to prevent any further security breaches. Additionally, regular security audits and checks can help to identify any potential loopholes in the security system, allowing organisations to take proactive measures to ensure their assets remain secure (Narayanan & Lee, 2022).
- **Well-defined roles and responsibilities:** Well-defined roles and responsibilities of individual employees are useful in getting employees to be more proactive and take higher precautions for information security. Clear penalties for information security violations in organisations encourage individuals to comply with information security policies. Previous studies have consistently shown that employees who are held accountable for a specific action behave in a socially acceptable manner. Accountability positively impacts employee compliance by increasing positive employee attitudes to avoid unacceptable behaviours and encouraging compliance with IT security policies (Assefa & Tensaye, 2021).

### 2.3.9 Cybersecurity culture

According to (Georgiadou et al., 2022), cybersecurity culture was first defined by Dhillon in 1999 as "the totality of human traits, including actions, attitudes, and beliefs, that have an impact on an organisation's digital information security and that relates to the safeguarding of all types of information inside an organisation". This means that cybersecurity culture encompasses not only the technical aspects of data protection but also the social and behavioural aspects, such as how people interact with each other and the technology they use.

The literature has demonstrated that knowledge of management and employees is critical in shaping cybersecurity culture. In a study by Reegård, Blackett & Katta (2020) Reegard, the authors list five things that affect how people behave when it comes to information security: a lack of understanding, a lack of desire, erroneous perceptions of risks, malicious behaviours, and inappropriate technology related usage. The study claims that minimising security threats brought on by insiders in the organisation is key to mitigating security risks and that one weakness is attitudes towards cybersecurity in the sense that cybersecurity is often seen as a technical matter to be handled by the company's IT department or its chief information officer (CIO).

#### 2.3.9.1 Organisational climate

Gross et al. (2020) explain that organisational climate refers to the company's total culture, which uses institutional, social, and psychological techniques to urge employees to abide by security standards. It puts a clear emphasis on modifying employees' behaviour.

According to research on organisational climate, higher management has less of an impact on employee behaviour than the immediate supervisor. Although senior management is key to establishing policies, processes and procedures for the whole organisation, lower levels of the organisation frequently implement those policies and processes. Usually, this takes the form of supervisor discernment in upholding routine procedures and enforcing policies (Gross et al., 2020).

#### 2.3.9.2 Management support, leadership, or involvement

The support and leadership of top and bottom management are the most discussed factors, particularly when it comes to maintaining a positive security culture. Top management, including its security culture, sets the tone for the entire company, including its security culture. When top management is committed to security, their actions and words are more likely to be taken seriously by other employees and managers. This commitment and support are essential for a strong security culture (Uchendu et al., 2021).

Support from top management relates to the actions of senior management and the board level to understand information security policies, advocate for organisational security, and prioritise security initiatives throughout the organisation. Management is

involved in influencing employee beliefs, attitudes, and behaviours to favour security compliance (Gross et al., 2020).

According to Reegård, Blackett and Katta (2020), management support can take many different forms, including managing and monitoring the cybersecurity function, status, and work. It can also take the form of financial investments in initiatives and a commitment to cybersecurity. The success of cybersecurity initiatives is significantly influenced by management support and cybersecurity levels of authority and their relationship with one another. This is crucial for establishing and maintaining a cybersecurity mindset within an organisation.

Cybersecurity authority levels are generally a group of stakeholders who ensure the survival of the organisation at large. They also help to ensure the security of the organisation's IT infrastructure and systems, as well as the safety of data and information. They are responsible for setting policies and procedures to ensure the organisation's IT systems and data are secure and compliant with applicable policies and guidelines (Lehto & Limnéll, 2021).

As illustrated in Figure 2.2, each of these cybersecurity authority levels has different responsibilities regarding information security.

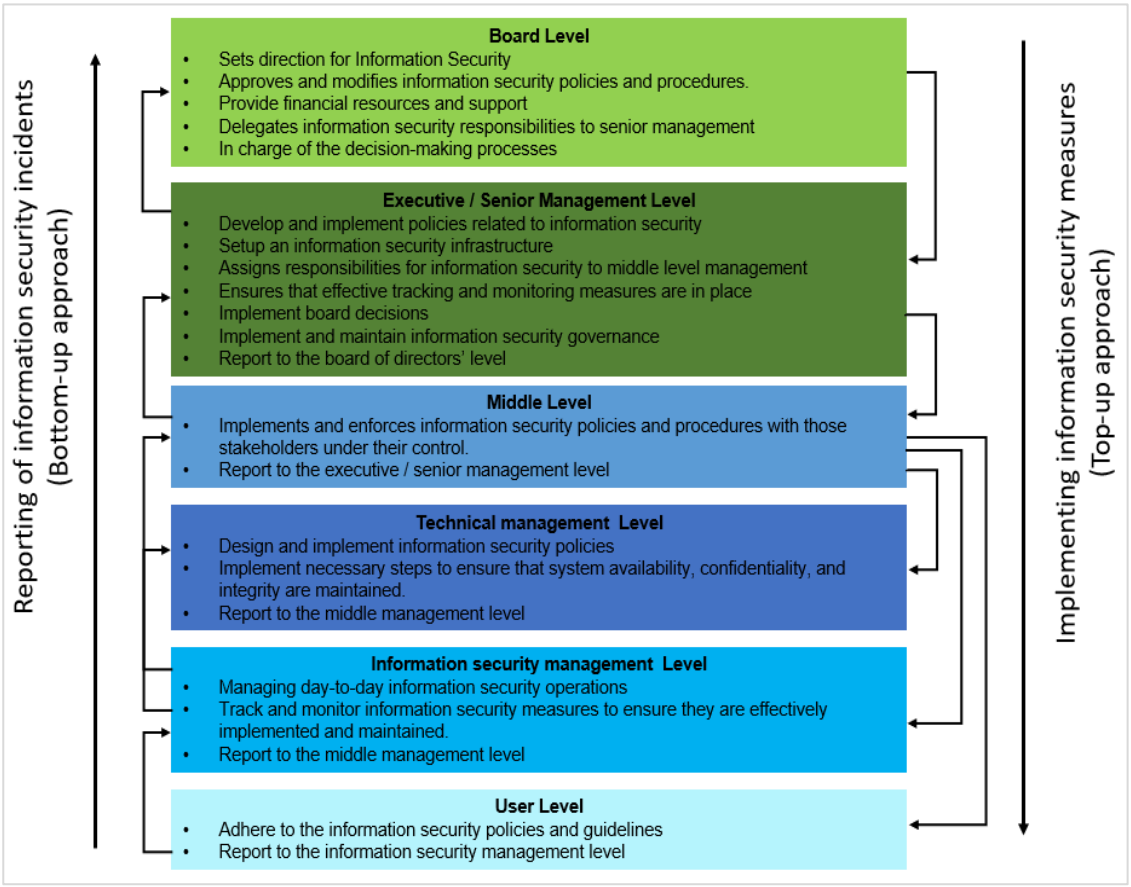



*Figure 2.2 Cybersecurity Authority Levels*

Source: Adapted from Kritzinger & Smith (2008)

### 2.3.9 Cybersecurity body of knowledge

A cybersecurity body of knowledge is formed when relevant information from various sources is gathered together for use as a guideline for securing data. This body of knowledge is useful in identifying risks, creating standards, and developing data protection strategies. It is an essential resource for improving the security of information systems (Rashid et al., 2018).

The proposed common body of knowledge is divided into system security, infrastructure security and software and platform security, as outlined below.

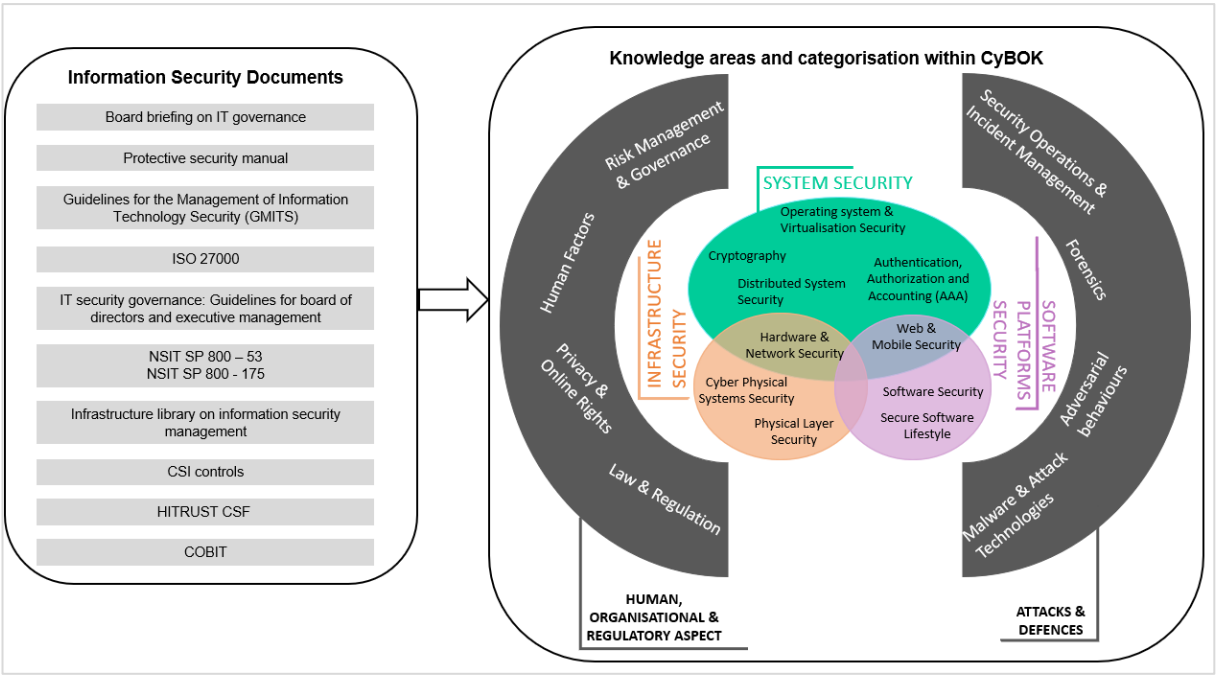



*Figure 2.3 Classification of CyBOK Knowledge Areas*

Source: Adapted from Rashid et al. (2018)

Table 2.2 provides an overview of the essential knowledge areas for developing and maintaining cybersecurity protocols.

*Table 2.2 An outline of the knowledge areas*

| | |
|---|---|
| **Human, Organisational and Regulatory Aspects** | |
| Risk Management and Governance | Organisational security controls and security management systems, including standards, best practices, and strategies for assessing and mitigating risk. |
| Law and Regulation | International and national legal and regulatory standards, compliance obligations, and security ethics, including data protection and the development of cyber warfare doctrines. |
| Human Factors | Useful security, cultural and behavioural elements that affect security, a culture of security and awareness, as well as the effect of security policies on user behaviours. |
| Privacy and Online Rights | Personal information protection techniques, such as communications, applications, and discoveries from databases and data processing. Other systems which support online rights are also included, including those that deal with filtering and circumvention, covertness, electronic voting, and security in payment and identification systems. |
| **Attacks and Defences** | |
| Malware and Attack Technologies | Technical information about distributed malicious systems and exploits, along with related methods for discovery and analysis. |
| Adversarial Behaviours | The motivations, behaviours, and techniques utilised by perpetrators, including malware distribution chains, channels of attack, and transfer of money. |
| Security Operations and Incident Management | Establishing, running, and maintaining secure systems, as well as identifying, handling, and responding to security incidents and gathering and utilising threat intelligence. |
| Forensics | Gathering, analysing, and reporting digital evidence in support of an occurrence or illegal activity. |
| **Systems Security** | |

| Human, Organisational and Regulatory Aspects | |
|---|---|
| Cryptography | Core cryptographic building blocks, newly developed algorithms, ways for analysing them, and the protocols that utilise them. |
| Operating Systems and Virtualisation Security | Mechanisms for protecting operating systems, enabling safe hardware abstraction and resource sharing, including isolation of multi-user systems, secure virtualisation, and security of database systems. |
| Distributed Systems Security | Security procedures for large-scale coordinated distributed systems, including aspects of secure consensus, time, event systems, peer-to-peer systems, clouds, multi-tenant data centres, and distributed ledgers. |
| Authentication, Authorisation and Accountability | Identity management and authentication technologies, as well as architectures and tools to support authorisation and accountability in both isolated and distributed systems, are covered in this section. |
| **Software and Platform Security** | |
| Software Security | Known types of programming defects that result in security bugs, as well as approaches for preventing such defects - through both better coding practice and improved language design as well as methods, tools, and techniques for detecting such defects in existing systems. |
| Web and Mobile Security | Web application and service distribution across platforms and frameworks related issues, such as the various development paradigms and security methods. |
| Secure Software Design and Development | The application of security software engineering techniques in the whole systems development lifecycle resulting in software that is secure by default. |
| **Infrastructure Security** | |
| Network Security | The implementation of security software engineering techniques throughout the whole system development lifespan which leads to the software that is secure by default. |

| Human, Organisational and Regulatory Aspects | |
|---|---|
| Hardware Security | Security in the development, implementation and deployment of both general-purpose and specialised hardware, including reliable computing methods and randomisation generators. |
| Cyber-Physical Systems Security | Security issues around cyber-physical systems, including IoT and industrial control systems, attacker models, safe-secure designs, and infrastructure security on a wide scale. |
| Physical Layer Security | Physical layer security concerns and restrictions, such as those related to radio frequency encoding and transmission methods, unintentional radiation, and interference. |

Source: Adopted from Rashid et al. (2018)

### 2.3.10 Insider threats

It is argued in Dash and Ansari's (2022) study that even though the organisation might have the most up-to-date technology in terms of firewalls, intrusion detection, and intrusion prevention systems, they are ineffective if the insiders or human factor of an organisation do not take measures to safeguard both their own systems and those of the organisation. In the realm of information security, the human factor is considered to be the most unpredictable vulnerability. It is characterised by being the most difficult variable to control. Organisations should address the human factor by assessing the security behaviour of individual staff members and ensuring that they have the right level of commitment to the policies of information technology (Alotaibi, Furnell & Clarke, 2019).

In this study, three types of insiders (malicious, compromised, and careless) and two non-compliance (intentional and unintentional) behaviours are explored to understand essential elements required to develop an awareness model to assist with mitigating risks related to security policy compliance (Saxena et al., 2020):

- **Malicious insider (intentional):** This threat refers to a current or former employee, contractor, or business partner who has or had authorised access to the organisation's information or information systems. This insider is aware of weak security policies and security awareness gaps within the company and then intentionally abuses access to credentials to steal information for personal or financial benefit. In this case, the employee can sell confidential information to someone outside the company.
- **Compromised insider (unintentional):** Credentials are targeted through compromised insiders using social engineering in order to obtain access to confidential business assets, data and information. Users are usually trapped through hyperlinks, multifactor authentication, lack of awareness or other means that users can easily overlook.
- **Careless insider:** This insider usually does not pay attention to the company's security practices and unintentionally leaks confidential business assets, data and information to outsiders or hackers.

Figure 2.4 shows types of insider threats and non-compliance behaviours with a summary of each type of insider

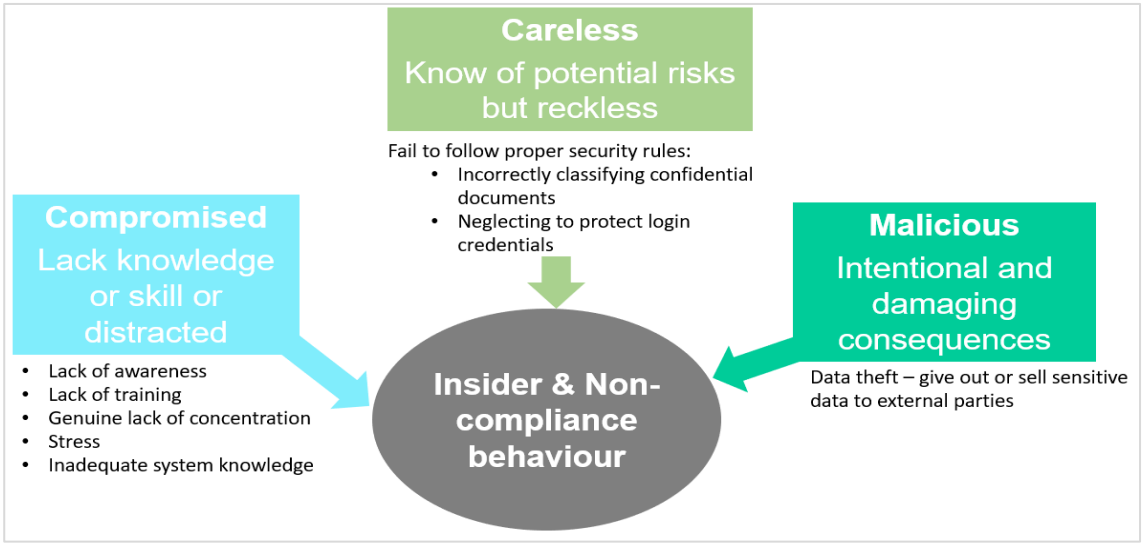



*Figure 2.4 Insider Threats and Compliance Behaviours*

The petroleum industry must recognise the significant risks posed by insider threats and take proactive measures to mitigate them effectively. Addressing malicious, compromised, and careless insiders is vital to protecting the industry's sensitive data, maintaining compliance with regulations, and upholding the industry's reputation and resilience in the face of evolving cybersecurity challenges. By investing in robust security practices, fostering a culture of security awareness, and implementing advanced security technologies, the petroleum industry can better safeguard its assets, maintain business continuity, and safeguard its position in the global energy landscape.

## 2.4 Chapter Summary

This section sought to provide organisations with an overview of cybersecurity, its risks, and methods for detecting and preventing these threats to assist them in making informed decisions and protecting themselves. Organisations need to know about social engineering tactics in order to educate their employees about the risks associated with it, such as clicking on suspicious links.

Cybersecurity is an ever-evolving field, with new threats and vulnerabilities emerging regularly. As such, the petroleum retail sector must continuously update and improve its IT security policies, conduct regular risk assessments, and implement the latest technological solutions to stay ahead of cyber adversaries.

Social engineering demonstrates the need for organisations to educate their workers regarding social engineering and security best practices (Aldawood & Skinner, 2019)and as a means of achieving this:

- It is important for organisations to invest in security measures and systems that can detect and block malicious activities from entering their networks or gaining access to the company's buildings and systems.
- Organisations should also have clear policies in place to ensure employees understand the risks and are aware of the appropriate measures to take if they receive a suspicious e-mail. Regular security audits can also help to identify any gaps in the organisation's security system.

- Organisations should regularly review existing security protocols, stay updated with the latest security developments and use the best tools available to protect their data and

systems. Companies should also invest in employee training programs to ensure that everyone

- Organisations need to ensure that employees are properly trained and understand the risks of social engineering to reduce social engineering attacks.

# CHAPTER 3
# THEORETICAL FRAMEWORKS

## 3.1 Introduction

Research dissertations in cybersecurity have considered a variety of theories and frameworks, and this study considers the five main technology adoption models: the Diffusion of Innovation Theory (DOI), the Technology Acceptance Model (TAM), the Social Cognitive Theory (SCT), the Unified Theory of Acceptance and Use of Technology (UTAUT) and the Technology-Organisation-Environment (TOE) framework. Each of these models brings valuable insights into understanding how individuals and organisations adopt and use technology, including IT security policies.

## 3.2 Diffusion Of Innovation Theory (DOI)

Rogers (1931-2004) formulated the theory of diffusion of innovations (DOI). Rogers (2003) defined diffusion as the process by which an innovation is communicated over time by members of a social system through certain channels. It is, therefore, viewed as a form of communication in which participants exchange information for the purpose of gaining mutual understanding. A new idea in a message gives diffusion its distinctive character, as an element of uncertainty is involved. Rogers (2003, p. 9) defines uncertainty as the degree to which several alternatives are perceived relative to an event occurrence. He described the DOI as a "process for reducing uncertainty" and suggested attributes of innovations that could lead to fewer uncertainties. DOI is primarily based on the characteristics of the technology used and how the users perceive the innovation.

An organisation is a much more complex entity than a single individual. Based on Rogers' vantage point, innovation could be considered a communication process using various channels within the social system (Amini, 2023). Arundel, Bloch and Ferguson (2019) defined the concept of innovation as the new idea, improvement, or enhancement of a new or existing product, technology, or process (or a combination of those products and processes) that differs significantly from the previous products or processes of the unit, and that has been made available to potential users (product) or has been used (process). (Amini, 2023)argues that three factors influence the adoption of innovation in an organisation. This refers to the individual characteristics of the leadership (attitude toward change in the organisation), the internal characteristics of the organisational

structure (centralisation, complexity, interconnectedness, number of employees, and organisational slack), and the external characteristics (the openness of the organisation's system).

Several factors influence the diffusion of innovations in society, such as relative advantage, compatibility, complexity, trial ability, and observe ability (García-Avilés, 2020):

1. **Relative advantage** refers to the degree to which an innovation is perceived as better than the idea it replaces. There is often a positive effect of relative advantage on innovation diffusion. If an innovation provides a clear benefit over the previous idea, people are more likely to adopt it quickly. This is because they understand the value it offers and how it will make their lives easier.
2. **Compatibility** refers to the degree to which an innovation is perceived to be in harmony with existing values, prior experience, and needs of potential adopters. Compatibility is also a significant factor in determining the speed of adoption of an innovation. It has been found that innovations that are compatible with the norms and values of individuals or with the norms of a social system spread more rapidly than innovations that are incompatible.
3. **Complexity** refers to the degree to which an innovation is perceived as relatively difficult to use and comprehend. Diffusion is usually negatively affected by complexity. Thus, a more complex innovation has a lesser chance of becoming widely accepted by society.
4. **A trial ability** can be defined as the degree to which an innovation may be examined and tested on a limited basis. This can be done either in a laboratory or a real-world setting, allowing the organisation to gather feedback on the innovation before committing to a full-scale launch. This can help to identify potential problems or opportunities that can be addressed before the launch.
5. An innovation's **observed ability** relates to the degree to which the results of the innovation are visible to others. Research suggests that people are more likely to adopt an innovation if they see it being used by others and if it is visible in its benefits.

Among all these five characteristics, relative advantage, compatibility, and complexity significantly impact the adoption rate of innovations. The perception of users in relation to an effective innovation promotes its adoption. Additionally, if an innovation is compatible with existing values and norms, it is more likely to spread rapidly. On the other hand, complexity negatively affects diffusion, as people are less likely to adopt innovations that are difficult to use and comprehend.

Overall, these factors play a crucial role in determining the success of innovations in society. In the context of cybersecurity, the DOI could help with understanding how various security measures or technologies are adopted across different user groups or organisations.

## 3.3 Social Cognitive Theory (SCT)

Albert Bandura initiated the Social Cognition Theory (SCT) in 1986 as the Social Learning Theory (SLT). The theory focuses on the idea that people learn from their environment by observing and imitating the behaviours of others. The SCT theory also considered the role of cognitive processes such as attention, memory, and motivation in learning. Ketidakpatuhan et al. (2018) describe social cognitive theory (SCT) as a theory based on personal, environmental, and behavioural factors that interact to predict group and individual behaviour. The founder Bandura (1989) argues that behaviour cannot change the environment as easily as it is influenced by the environment unless behaviour first changes itself and that what people think, believe, and feel influences their behaviour. SCT can be used to investigate decision support and behaviour in cyberspace. As such, it should be able to back a strong security framework that investigates typical user actions. For instance, a fundamental component of SCT is the investigation of the influence of self-efficacy on decision-making and cyber behaviour. Self-efficacy is a kind of self-evaluation that plays an important role in individual behaviour (Maalem Lahcen et al., 2020).

Three individual cognitive elements are influenced by the surrounding environment and are, according to Beauchamp, Crawford and Jackson (2019):

1. **Observational learning:** Individuals are more likely to engage in a desired behaviour if they observe others engaging in it and receiving positive reinforcement. This is because people learn by imitation and tend to copy the

behaviour of others. When they see someone else being rewarded for the desired behaviour, they are more likely to imitate it in order to receive the same rewards.

2. **Outcome expectations:** Individuals are more inclined to engage in a desired behaviour if they feel the rewards exceed the risks. People are more likely to engage in a behaviour if they feel that the resulting outcome will be beneficial. For example, if a person believes that the reward of getting a promotion at work outweighs the risk of working hard, they are more likely to put in the extra effort.
3. **Self-efficacy:** Individuals are more likely to engage in a desired behaviour if they believe they have the necessary skills and capabilities. When a person has a higher level of self-efficacy, they are more likely to believe that they can successfully complete the task, and as a result, they are more likely to actually take action and do it.

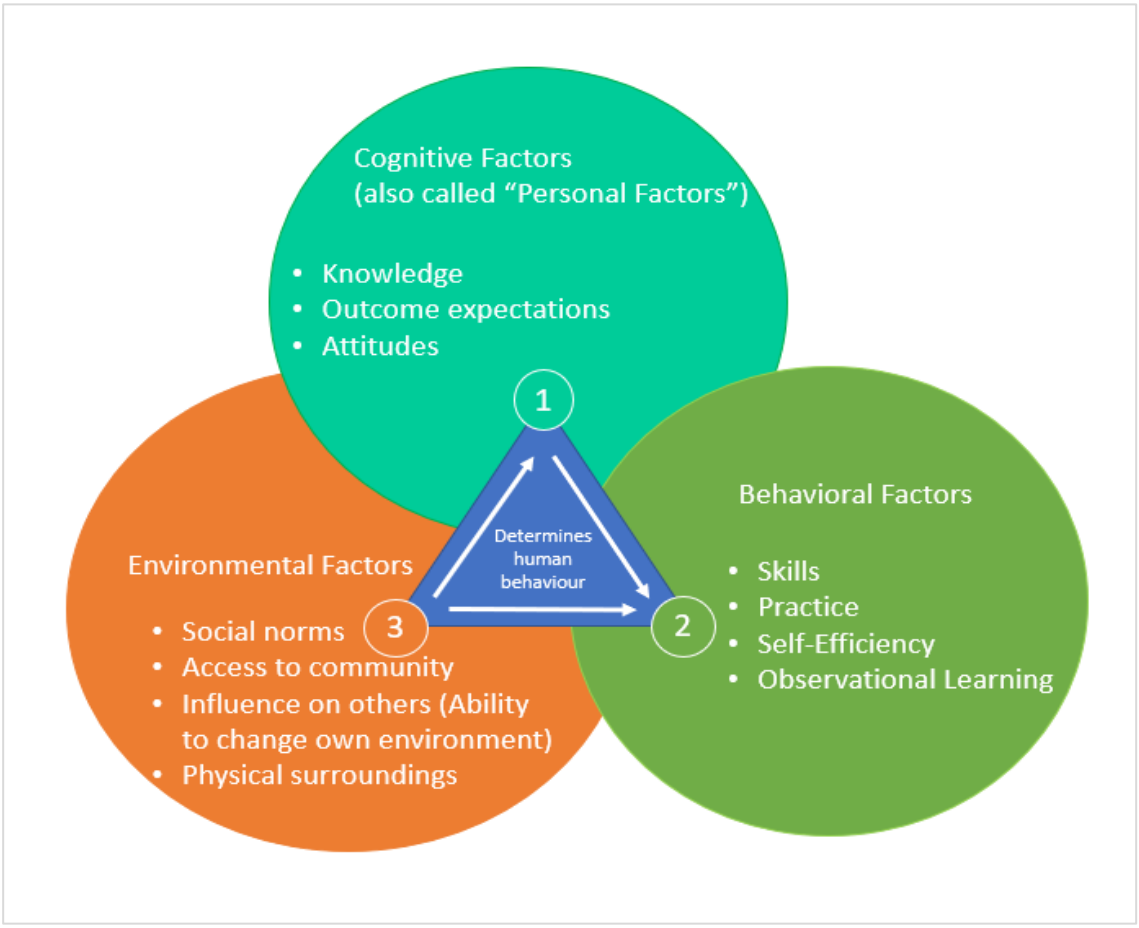



*Figure 3.1 Social Cognition Theory*

Source: Adapted from Maalem Lahcen et al. (2020)

By understanding how self-efficacy influences decision-making and cyber behaviour, SCT can help to better secure cyberspace by providing insight into typical user actions and how they might be manipulated. This, in turn, can lead to the development of stronger security frameworks and practices, which can help protect users from potential threats.

SCT also has its limitations. For example, SCT does not account for all possible user actions and decision-making approaches. For instance, in the case of self-efficacy, SCT may not accurately predict how an individual will behave in a given situation because it is based on the idea that the environment determines behaviour and does not encapsulate the individual's internal motivations, beliefs, or values.

## 3.4 Technology Acceptance Model (TAM)

Davis (1987)introduced TAM, which is a cognitive theory based on the theory of reasoned actions (TRA) and the theory of planned behaviour. Davis (1987) argues that lack of user acceptance has long been a significant barrier to the success of information system initiatives. As a result, TAM has been developed in order to address:

1. The reasons why end users accept or reject information systems
2. How the design features of the system affect user acceptance.

According to Surendran (2012), TAM demonstrates a relationship that suggests an individual's general attitude about using a particular system is considered a crucial factor in determining whether or not someone actually uses the system. In turn, attitude toward using is a result of two major beliefs, which are as follows:

1. **Perceived usefulness** refers to the user's subjective likelihood that using a particular system/technology will improve a user's job performance.
2. **Perceived ease of use** refers to the extent to which a user believes using a system or technology will not require any physical or mental effort.

IT acceptability and utilisation is the most essential aspect of information systems research and implementation. Even though businesses have made substantial investments in the ongoing development of IT hardware, software, and infrastructure, a productivity paradox is emerging due to a poor awareness of how IT is being utilised; this situation calls for immediate improvement (Park & Park, 2020).

Figure 3.2 shows the casual interrelationships between system design features, perceived usefulness, perceived ease of use, attitude toward using and actual usage behaviour.

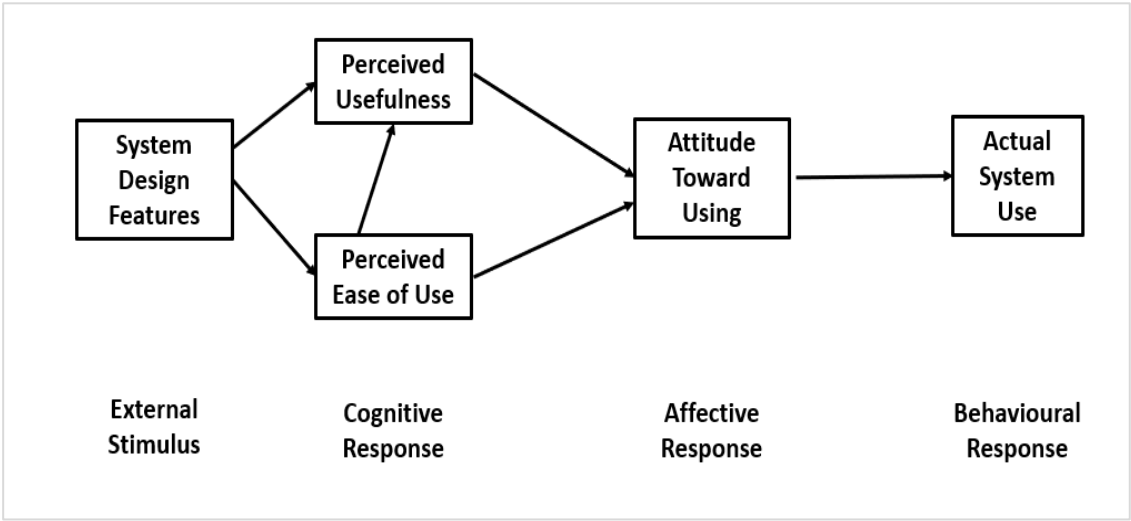



*Figure 3.2 Technology Acceptance Model (TAM)*

Source: Davids (1987)

The subjective norms (external influences) that could impact technology acceptance were not accounted for in Davids's (1987) TAM model. The initial study did not demonstrate that attitudes significantly influenced behavioural intentions. Worthington and Burgess (2021) looked at the influence of external factors, such as subjective norms, on technology acceptance. The study illustrated that subjective norms significantly affected technology acceptance and that the TAM model needs to be expanded and modified to incorporate these external factors.

Because TAM focuses on individual users, it does not consider other elements affecting technology acceptance, such as cost, system capabilities, social factors (language, skills), cultural factors, gender, alternative systems, and group usage. These elements are essential to understanding how well a technology will be accepted by a user population. For instance, if the cost of the technology is too high, it may limit its usage even among those who are otherwise willing to use it. Additionally, social and cultural factors can shape how an individual interacts with technology and might even be a factor in their decision to use or not use it.

## 3.5 Unified Theory of Acceptance and Use of Technology (UTAUT)

According to Momani (2020), the Unified Theory of Acceptance and Use of Technology (UTAUT) is a widely recognised framework within the context of technology usage and adoption formulated by Venkatesh et al. in 2003. Momani (2020) additionally indicated that UTAUT seeks to clarify and estimate the factors that influence individuals' decisions regarding adopting and utilising technology.

The framework integrates elements from multiple preceding models of technology adoption, including the Innovation Diffusion Theory (IDT), Technology Acceptance Model (TAM), and Theory of Reasoned Action (TRA) (Etim, 2021). UTAUT highlights various types of key factors that contribute to the acceptance and use of technology.

1. **Performance Expectancy** refers to the user's perception that technology will improve their job performance or deliver some advantage. In the Technology Acceptance Model (TAM), it is similar to perceived usefulness (Gangwar, 2020).
2. **Effort Expectancy**: This component represents the user's perception of the technology's ease of use and the effort necessary to learn and operate it. In TAM, this is similar to perceived ease of use (Izyaty et al., 2019)
3. **Social Influence**: Social factors influence technology uptake significantly. Social influence includes subjective norms and the views of influential peers or colleagues (Roberts et al., 2021).
4. **Facilitating Conditions**: These are the resources and support available for using technology, such as assistance in technology, training, and infrastructure (Park, Lee & Yi, 2011).

5. **Gender**: The adoption of technology can be influenced by gender, as males and females may have distinct perceptions of technology (Shaouf & Altaqqi, 2018).
6. **Age**: The impact of age on technology adoption can vary since various generations may have varied levels of knowledge and comfort with technology. Older individuals often face more obstacles when embracing and utilising technology than younger individuals (Wilson, 2018).

UTAUT does not emphasise external environmental factors, such as economic conditions, legislative changes, or market dynamics, that can greatly influence the adoption of technology in specific situations.

UTAUT primarily emphasises rational and cognitive aspects, such as the perceived usefulness and ease of use. However, it does not adequately address behavioural or social elements, which can also significantly influence decisions on technology adoption.

## 3.6 Technology-Organisation-Environment (TOE)

This study is underpinned by the TOE framework; the subsection that follows explains what the TOE framework is, why it is a crucial part of this study, and what it means for this study.

The TOE framework is used in this study as a lens to assist in examining and understanding the factors that influence IT security policy compliance and adoption within the petroleum retail sector and the elements required to develop an awareness model to encourage the use of IT security policies. Considering the interplay of technology-related, organisational, and environmental factors, the TOE framework provides a comprehensive perspective on how and why organisations adopt specific technological innovations or practices, such as cybersecurity measures.

### 3.6.1 Background and context of TOE

Technology-Organisation-Environment framework (TOE) is an information systems (IS) theory that addresses how decisions about the adoption of IS are made. It posits that organisational traits, environmental circumstances, and already-existing technologies interact to impact adoption and usage choices

Deelert, Jaturat and Kuntonbutr (2020) refer to the TOE framework developed by Tornatzky in 1990 to study the technology adoption of an ERP Management system and IT services and products at the organisational level. A study by Dube, Van Eck and Zuva (2020) stated that TOE consists of three fundamental components: technology, organisation, and environment. The framework considers the external and internal influences on an organisation and the relationship between an organisation and technology.

Organisations use the TOE framework to better understand the complexity of technology and policy adoption. It can help organisations identify potential risks and opportunities that can influence technology adoption and compliance (Dube, Van Eck & Zuva, 2020).

The following table summarises the factors that have been explored for each component of TOE in this study. To achieve the desired results of the research problem, each component of TOE has been carefully evaluated, considering all the relevant factors to allow for accurate and reliable outcomes.

### 3.6.2 TOE Framework for IT Security Usage, Compliance and Adoption

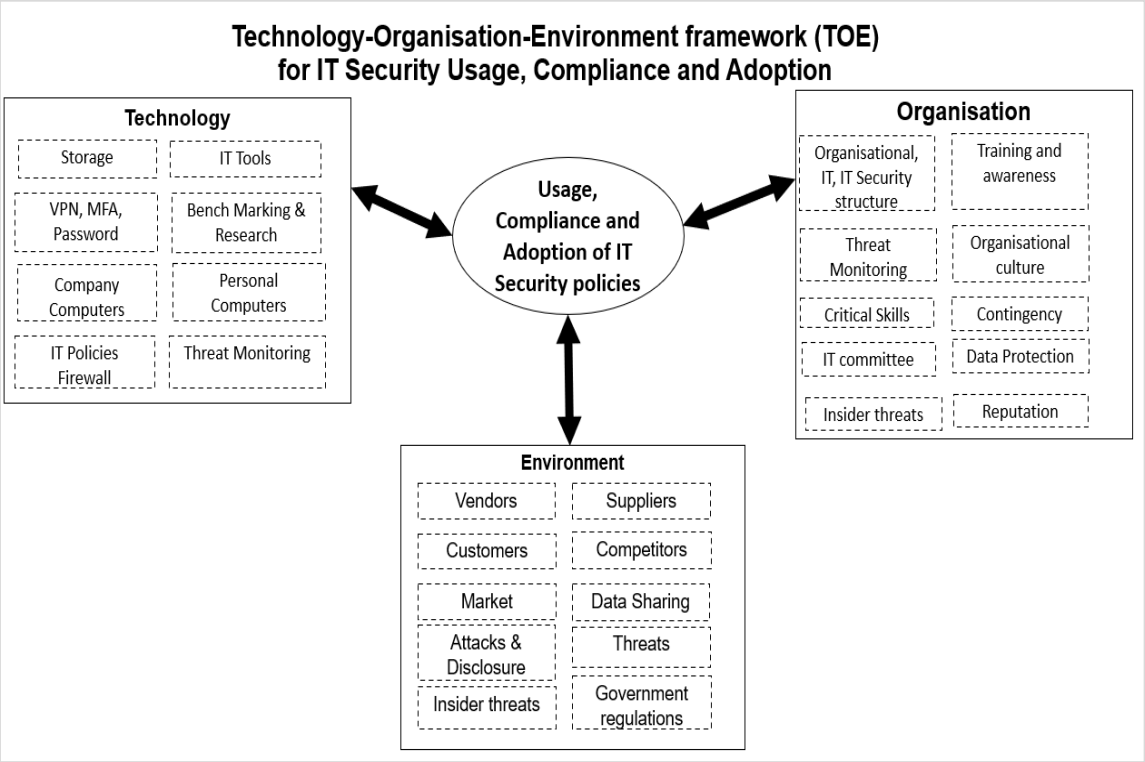


*Figure 3.3 TOE Framework*

Source: Adopted from Wallace et al. (2021)

### 3.6.3 TOE Dimensions and Considerations

A summary of the TOE dimensions and a description and considerations of each dimension are given in Table 3.1. Each dimension is designed to measure the understanding, insights and application of the TOE framework in the context of cybersecurity.

*Table 3.1 Considerations for TOE*

| Dimension | Description | Considerations |
|---|---|---|
| **Technology** | Technology is used to study factors that affect the acceptance of IT policies and technology strategies that are meant to drive usage and policy compliance. Technology influences usage decisions based on its characteristics, ease of use, and availability. | **Policies and Standards:** controls, storage location and approval procedure, Password protection, Multifactor authentication, VPN |
| | | **IT Tools**: Servers, network, applications, configurations, patches, Monitoring and Threat Monitoring |
| | | **Firewall:** Network Threat Prevention; Application and Identity-Based Control; Hybrid Cloud Support; Scalable Performance |
| | | Benchmarking and Research |

| Dimension | Description | Considerations |
|---|---|---|
| | | **Computers and Mobile Devices:** Company and personal devices and related configurations, controls, policies, and patches |
| **Organisation** | Organisation is examined to understand internal factors such as personnel, organisational structure, organisational culture, management support, communication processes and size and how they could affect usage decisions. | **Organisational structure:** Training and awareness, Critical Skills (CIO turnover, Staff Skills), IT committee, IT security team structure |
| | | **Data protection and Contingency: D**ata backups, DR, business continuity plan |
| | | **Organisational culture:** Training, whistle-blower, end-user involvement |
| | | **Threats:** Insider threats (view of threats related to insiders), technological threats |
| | | **Reputation** |
| **Environment** | Environment is studied to understand external factors that impact the decision to use the technology, such as industry characteristics, government | **Threats:** Attacks, Disclosure |
| | | **Market:** Market trends, Competitors |

| Dimension | Description | Considerations |
|---|---|---|
| | regulations, customers, and partners, and how these external forces influence technology and compliance strategies. | **Data sharing:** customers, suppliers, vendors and contractors |
| | | **Government regulations** |

Source: Adopted from Wallace et al. (2021)

## 3.7 The adoption of the TOE model

This study adopts the TOE framework, and the framework is well-suited for addressing IT security compliance challenges. This framework has been adopted because it is a holistic, comprehensive, and dynamic framework for organizational use (Hasan et al., 2021). It is a robust framework that integrates internal (technology and organizational) factors and the external environment to shape IT security adoption and compliance.

According to (Hale & Gamble, 2019), compliance with IT security standards involves more than just implementing technical solutions; it also requires alignment with organizational strategies, structures, cultures, and external regulatory requirements. This is because IT security standards require a comprehensive approach that covers all aspects of an organisation's operations from technology to people to policies to suppliers and vendors and to government regulations to enhance security posture, and efficiently address potential risks.

## 3.8 Chapter Summary

This chapter explored several key theoretical frameworks that play a crucial role in understanding the adoption and acceptance of technology. These frameworks encompass diverse perspectives, each shedding light on specific aspects of the complex process of integrating new technologies.

The highlighted frameworks include:

- Diffusion of Innovation Theory (DOI) by Rogers (1931-2004), which explains the process of how an innovation is communicated and adopted over time through social systems.
- Social Cognitive Theory (SCT) by Bandura (1986), which focuses on the role of cognitive processes, social environment, and individual factors in shaping behaviour.
- Technology Acceptance Model (TAM) by Davis (1987), which examines the reasons why end-users accept or reject information systems based on their perceived usefulness and ease of use.
- Unified Theory of Acceptance and Use of Technology (UTAUT) by Venkatesh et al. (2003), which integrates elements from multiple models of technology adoption to explain the factors that influence individuals' decisions to adopt and use technology.
- The Technology-Organisation-Environment (TOE) developed by Tornatzky in 1990 which is a lens used in this study to examine the interplay of technology, organizational, and environmental factors that influence IT security policy compliance and adoption in the petroleum retail sector.

In this chapter, key concepts, principles, and applications of each framework were explored, illustrating how the study can utilize these perspectives to analyze and predict IT security adoption patterns. Taking these frameworks into account together provides guidance in selecting the most appropriate framework that will provide a comprehensive understanding of how IT security policies are adopted and used in various contexts.

# CHAPTER 4
# RESEARCH DESIGN AND METHODOLOGY

## 4.1 Introduction

This chapter is intended to give an in-depth description of the research design and methodologies required to address the research questions and accomplish the objectives of the study. In order to ensure the validity and reliability of the research, the chapter describes and discusses the context of the research philosophy, research design, research approach, data gathering strategies, and data analysis methodologies.

In order to address the research problem effectively, the appropriate research methods need to be selected. Thus, this study has adopted the research onion proposed by Saunders et al. (2019), as illustrated in Figure 4.1 below. The onion shows different methods, strategies and approaches used in this research under each of the six main layers of the research onion.

Saunders' research onion has been used as a guide to help analyse the use of IT security policies, compliance, and adoption in the petroleum retail sector and then formulate a model to improve compliance and adoption of IT security policies.

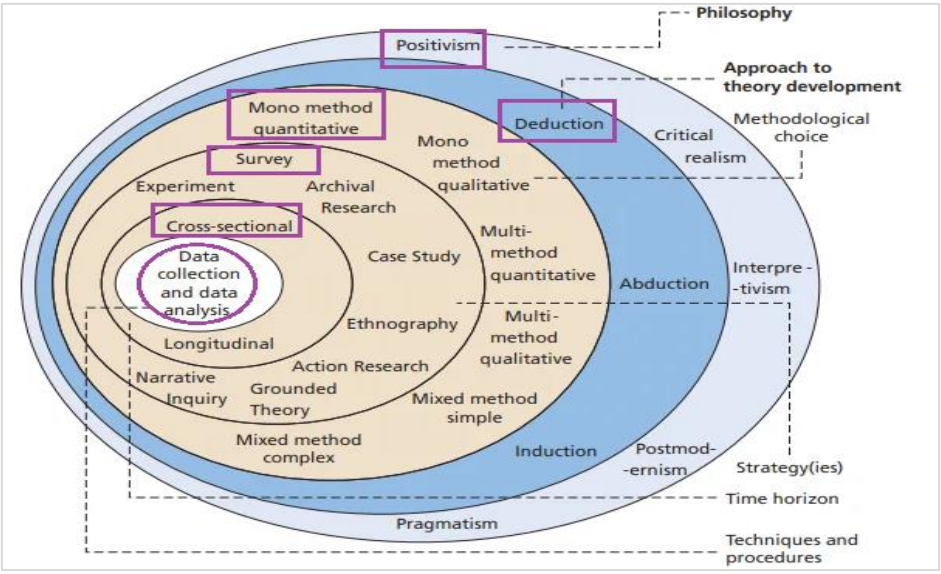



*Figure 4.1 Research onion*
Source: Saunders et al. (2019:108)

## 4.2 The Research Philosophy

A research philosophy serves as a foundational framework that guides the researcher's approach to understanding and studying the world. It encompasses fundamental beliefs and assumptions about the nature of reality, the role of the researcher, and the methods through which knowledge can be acquired (Galliers, 1991). The selection of the research philosophy in this study significantly influenced the research design, methodologies, and the interpretation of the results.

Three primary research philosophies exist, each linked to distinct methodologies for investigation:

### 4.2.1 Interpretivism paradigm

Alharahsheh and Pius (2020) explain that in the interpretivism paradigm, humans create deeper meanings than physical phenomena:

- Interpretivism is more interested in in-depth variables and context-related factors. It assumes that humans cannot be studied in the same way as physical phenomena.
- Interpretivism considers the variations in cultures, situations, and historical periods that led to the formation of various social realities.
- In contrast to positivism, which tries to give clear, universal laws that can be generalised and applied to everyone, interpretivism strives to include richness in the insights obtained.

Qualitative researchers advocate for the interpretivism paradigm as they argue that human beings perceive things in diverse ways, and the investigation methods should accommodate this differentiation.

### 4.2.2 Positivism paradigm

Al-Ababneh (2020) defines positivism as a philosophical and research paradigm that emphasises the objective and empirical observation of phenomena. It is rooted in the belief that knowledge can be gained through systematic and scientific observation of the world and that an objective reality exists independently of our perceptions. According to

Karupiah (2022), positivism is associated with the idea that the scientific method, with its emphasis on empirical evidence and quantifiable data, is the most reliable means of acquiring knowledge.

Positivism stresses the importance of objectivity in research. It aims to minimise bias and personal interpretation, focusing on observable and measurable facts and is closely associated with quantitative research methods, where data is analysed using statistical techniques to identify patterns, correlations, and causal relationships (Park, Konge & Artino, 2020).

This research study follows a positivist paradigm, which implies that data was collected by questionnaires and then analysed quantitatively to draw conclusions. The researcher reached conclusions in an impartial and objective manner, and the findings have been generalized to the population.

### 4.2.3 Critical realism

Bukowska (2021) argues that the realist philosophy, also known as critical realism, is a philosophical perspective that acknowledges the existence of an external reality independent of human perception but recognises that our experiences and perspectives mediate our understanding of this reality. Additionally, critical realism seeks to go beyond simple empiricism or positivism by exploring the underlying structures and mechanisms that shape phenomena.

Critical realism is advantageous for research studies as it facilitates the integration of theory and data, thereby enhancing understanding of research processes and facilitating the discovery of new research avenues (Eriksson and Engström, 2021).

The research follows a positivist approach for the study due to the preference for a systematic, structured, and objective investigation of the research questions aligned with the study's aim and objectives. This approach allowed the researcher to draw reliable conclusions from the data obtained through rigorous and systematic methods. The researcher was also able to apply quantitative data analysis techniques, such as correlation and regression, to analyse the data.

## 4.3 Approach to Theory Development

The deductive approach is systematic and structured, as it involves testing specific predictions derived from the theory through empirical observations and data collection (Dudovskiy, 2019). The study aims to confirm or refute the initial theory regarding IT security policy compliance and adoption by moving from the general theory to specific predictions and data collection.

(Patel Mimansha & Patel Nitin, 2019) states that the inductive approach in involves starting with specific observations or evidence and then moving towards broader generalizations or theories. It focuses on identifying patterns, generalizing from specific examples, and developing theories based on observed phenomena .

Abductive approach seeks the most likely or plausible explanation for a set of observations or evidence, and it involves generating possible explanations and selecting the one that best fits the available data (Ren et al., 2018). Abductive reasoning is often used when there are multiple possible interpretations.

This research follows the deductive approach. The process began with a theory, or a general hypothesis related to IT security policy compliance and adoption. The researcher has examined this theory by conducting empirical observations and collecting data. The investigation transitioned from a broad scope to a more focused and precise approach during this process. The researcher has generated precise predictions or hypotheses derived from the theoretical framework, followed by the collection of empirical data to assess the validity of these predictions. The objective is to validate or disprove the initial hypothesis.

## 4.4 Research Approach

Mono-quantitative research methodology involves the use of numerical data to quantify attitudes, opinions, and behaviours. It also follows a deductive research method, which involves testing a hypothesis through the collection and analysis of data and also follows a descriptive non-experimental strategy (Rahman, 2016).

Quantitative research is a formal and systematic approach that uses experimental or non-experimental designs to obtain accurate measurements and discover relationships between variables within a population (Mohajan, 2020).

According to Branaghan et al. (2021), quantitative research collects and analyses numerical data to answer research questions using methods such as questionnaires, biometric research, correlational research, and experiments.

(Nassaji, 2020) explains that mono-qualitative research methodology aims to explore and understand the subjective experiences, perspectives, and meanings that individuals attribute to phenomena. Qualitative research is interested in the richness and depth of participants' insights, and it examines how social contexts, interactions, and cultural factors contribute to the creation and interpretation of phenomena (Campos & Hickey, 2022).

Qualitative research involves collecting non-standardized data. This can include open-ended interviews, observations, focus group discussions, or content analysis of texts and images (Ponce, Gómez-Galán and Pagán-Maldonado, 2022). Qualitative research prioritizes in-depth exploration and detailed insights of the context in which phenomena occur rather than generalizable findings applicable to a larger population (Liamputtong, 2023).

Whitehead (2020) talks about semi-structured interviews in qualitative research as types of interviews where the questions are open-ended and a two-way interaction, participants can expand on topics they believe to be essential as the talk develops in a conversational style where participants are free to ask follow-up questions to further discuss their answers.

According to (Sharma et al., 2023), in mixed-methods research, qualitative and quantitative research techniques are integrated into a single study by combining the benefits of qualitative and quantitative methodologies, this strategy aims to provide a deeper, more complex knowledge of the phenomena or research issue. While mixed methods offer the advantages of both approaches, integrating both qualitative and quantitative elements might necessitate knowledge of both domains, which could make the research design more complicated (Hewlett & Werbeloff, 2023).

In this study, a mono-quantitative method was adopted since it allows the opportunity to collect objective, numerical data that can be easily quantified and examined statistically, allowing for a more thorough investigation. Additionally, it is effective in

generating numerical data and offers the ability to generalise results from a larger sample population.

## 4.5 Research strategy and outcome

### 4.5.1 Survey Research

Surveys entail gathering information from a sample of people via standardized questionnaires or interviews. They can be conducted through face-to-face interviews, telephone interviews, online surveys, and paper-and-pen questionnaires. Surveys are essential for acquiring information about people's views, opinions, beliefs, behaviours, demographics, and other aspects and they can provide quantitative data that can be statistically analysed to find patterns or trends (Kennedy, Jensen & Jensen, 2022). This research strategy is efficient for collecting data from a large number of respondents and caters for various channels such as online, in-person and telephonically.

### 4.5.2 Experimental Research

This strategy involves manipulating one or more variables to observe the effect on another variable under controlled conditions. It allows researchers to establish cause-and-effect relationships (Stewart, 2022). For example, Baetu (2021) asserts that a researcher might conduct an experiment to test the effectiveness of a new drug by randomly assigning participants to either the experimental group (receiving the drug) or the control group (receiving a sample) and measuring the outcomes.

Experimental settings are frequently artificial environments produced by researchers that may not accurately mirror real-life events. As a result, experimental findings may not always be applicable in real-world circumstances.

### 4.5.3 Case Study Research

Case studies entail a comprehensive analysis of a particular person, group, organization, or phenomenon in the context of real-life situations in order to obtain a comprehensive understanding (Ndame, 2023).

Ndame (202) continues to explain that in order to get a thorough understanding of the case, researchers gather and examine evidence from a variety of sources, including documents, observations, and interviews. Case studies are useful for investigating

unique or uncommon cases, learning about complex processes, or providing practical examples to support theoretical ideas.

Findings from a single case might not be easily generalizable to a wider population, which is one of the primary drawbacks of case studies. It is difficult to generalize the findings due to the distinctiveness of each case.

### 4.5.4 Grounded Theory

The grounded theory method is a quantitative research methodology that is used to build conceptual frameworks or theories based on data analysis conducted through the systematic interpretation of the data. The method is particularly useful for exploring phenomena that are complicated or poorly understood (Akkaya, 2023).

According to  in contrast to traditional deductive research, which involves testing a hypothesis against empirical evidence, Grounded theory begins with data and grants theories to emerge from the data analysis process.

This research study has adopted a survey as the research method, which involves collecting data from a sample of 66 participants using a structured questionnaire or survey instrument. The survey method allowed the researcher to gather standardised and quantitative data efficiently, making it suitable for assessing specific research questions or hypotheses related to the improved IT security policy compliance and adoption. Additionally, the survey method allowed for a large sample size to be collected over a short period of time, which helped to increase the reliability and validity of the results making the data analysis process much simpler and more accurate.

## 4.6 Research time horizon

Alturki (2021) defines a time horizon as a specified and specific timeframe during which a study takes place, including the time when data was collected and analysed. Additionally, Alturki (2021) highlighted that a cross-sectional time horizon refers to a single snapshot taken over a specific period of time and facilitates capturing the direct correlation between causes and effects. In contrast, a longitudinal time horizon involves multiple snapshots taken over a set time and facilitates the capturing of changes and testing the consistency of conclusions over a long period.

This research study followed a cross-sectional time horizon because data was collected at a specific point in time, and there was not enough time to go back and revisit participants to test consistency and changes of conclusions over time. The use of this research technique was suitable for this study as it allowed the researcher to draw conclusions regarding the associations between variables based on the gathered data. In addition, a cross-sectional design allowed the researcher to accurately evaluate the impact of specific variables on research participants at a specific moment in time.

## 4.7 Data collection

The data collection for this research study follows a quantitative approach using closed-ended questionnaires. Closed-ended questions were chosen for convenience in online settings, making it easy for respondents to respond quickly with a key press or mouse click, reducing intellectual load. Connor and Reimers (2019) argued that closed-ended questions are more convenient to utilise in online settings due to their tendency to elicit responses that may be answered with a single key press or mouse click. Moreover, they impose less intellectual load on respondents. However, it is important to note that closed-ended questions have the potential to introduce bias into the obtained results. Closed-ended questions prompt speedier responses than open-ended questions.

TOE framework was used as a strategic approach to develop research questionnaires in order to study the adoption of cybersecurity policies and compliance. This helps to ensure a comprehensive exploration of the various factors that play a role in shaping an organisation's approach to cybersecurity. The researcher conducted the study with questionnaires amongst the petroleum retail sector employees and the manager/s in the dynamics of an email template, which lasted approximately 10 to 15 minutes to complete, and sampling was carried out until data saturation was reached; the sample consisted of technical and non-technical employees. Questionnaires allowed participants to open up about private matters often overlooked when interacting in face-to-face interviews and group dynamics.

Data was collected through questionnaires using Microsoft Forms. Questionnaires were sent to 100 non-technical employees, an IT Security Specialist, and the IT Manager. Data was stored in a secured folder where only the researcher could access the responses. Data collection was halted during the study when the results were convincing

enough to conclude that an effect was present or when it was extremely unlikely that the predicted effect was observed.

The researcher has used gathered information to produce data that one can transform into usable data to motivate a proposed awareness model to encourage Information technology security policy compliance and adoption.

*Table 4.1 Research questions and key outcomes*

| Research question | Research Question Description | Objectives | Subjects | Key Outcomes |
|---|---|---|---|---|
| SQ1 | What IT security controls or policies are in place to protect organisational information? | To determine IT security policies and controls that are in place to protect organisational information | IT managers, IT Employees, Non-technical managers and employees | Description of policies and controls for protecting information in an organisation |
| SQ2 | What organisational factors are used to promote IT security policy compliance and adoption? | To discover organisational factors used to promote IT security policy compliance and adoption | IT managers, IT Employees, Non-technical managers and employees | A List of factors influencing IT security policy compliance and adoption in the organisation |
| SQ3 | What challenges are experienced with IT security compliance in the organisation? | To discover challenges experienced with IT security compliance in the organisation? | IT managers, IT Employees, Non-technical managers and employees | A list of challenges related to IT security policies |

| Research question | Research Question Description | Objectives | Subjects | Key Outcomes |
|---|---|---|---|---|
| Main Question | How can an awareness model be developed to improve the use of IT security policies in the petroleum retail sector? | To develop an awareness model to improve the use of IT security policies in the petroleum retail sector? | IT managers, IT Employees | An awareness model<br><br>A list of essential elements required to develop an awareness model |

## 4.8 Data analysis – Statistical Analysis

This study used statistical analysis to collect, explore, summarise, and interpret data. Through this process, statistical techniques have been used to discover patterns, relationships, or insights within a dataset. A statistical analysis has been used to provide insight into data, draw conclusions, and assist decision-making.

Statistical analysis is defined as the analysis of data using statistical testing to examine a research hypothesis and involves systematic gathering and examination of extensive data sets to detect patterns and generate meaningful observations (Vandever, 2020).

The SPSS data analysis tool has been used to compare and analyse data, create data visualisation, and build relationships. The researcher has used the results from SPSS to draw meaningful insights and conclusions. The researcher of this study has transformed the data into written text before analysis can begin and has used the researcher's expert opinion to give meaning, order, and structure to the voluminous data collected from the Cape Town petroleum retail sector through interviews, observations, recordings, writings, and theories. In order to effectively handle, alter, edit, organise, and code the large amounts of data gathered from the petroleum retail sectors, the researcher has used a computer system, such as a laptop, with the necessary programs.

The researcher has used the modified structured data to draw findings and develop a model to encourage the usage of IT security.

## 4.9 Data Validation

Data validation is a critical step in quantitative research to ensure the accuracy, reliability, and integrity of the data collected. It involves a series of processes and checks to identify and rectify data errors, inconsistencies, and anomalies (Surucu & Maslakci, 2020). The researcher took measures to ensure that the survey questions were formulated clearly, unambiguously and aligned with the research objectives. A preliminary assessment of the questionnaire was carried out through pilot testing with a limited sample size in order to detect and address any potential concerns prior to the commencement of data collecting on a larger scale.

The respondents were supplied with a comprehensive explanation explaining the research objectives, the significance of the research, and the criticality of precise data collection.

The questionnaire data underwent a thorough assessment through closed-ended pilot testing with a small group similar to the target audience to identify any inaccuracies or missing values, which were then rectified or removed as necessary. A precautionary measure such as Google Drive and SharePoint was taken to create a backup of the processed dataset prior to commencing the analysis, ensuring that the work performed is safeguarded in the event that it becomes necessary to revisit the cleaned data at a later stage. While quantitative data does not lend to a traditional qualitative theme, the researcher has identified patterns or trends that were considered themes as a strategy to uncover insights and enhance data analysis. The researcher has assigned codes to data points that fall within each research question in order to structure categories that can be analysed in the quantitative research tool. After coding the data, the researcher imported the coded dataset into the SPSS analysis tool to explore, test hypotheses, and derive insights from the identified patterns.

## 4.10 Sampling/justification

Sampling is the process of selecting units (e.g., people, organisations, times) from a population of interest, studying these in detail, and then drawing conclusions about the larger population (Pandey & Pandey, 2015). The evaluator has collected data from a

subset of individuals – a sample – and used those observations to make inferences about the entire population. The investigations have been conducted at a petroleum retail company in Cape Town, South Africa.

This research has used a non-probability purposive sampling of convenience technique. This type of sampling implies that not every member of the population has the same chance of getting chosen when the samples are drawn (van Haute, 2020). This choice is because it is almost impossible to give all petroleum retail sectors and employees a chance to be part of the interview due to issues such as time, distance, budget, population size and other limitations.

The researcher intentionally targeted the petroleum retail company in Cape Town with a sample of IT and non-IT employees. Participants were sent an email invitation to participate in this study. IT employees were selected since they are usually the early adopters of IT security policies and systems and are required to comply with IT policies; they would be able to answer the closed-ended questions promptly without hesitation. Non-IT employees were selected because they are required to comply with IT policies and sometimes find it difficult to understand IT-related compliance requirements.

The researcher has drawn conclusions for a larger population of the petroleum retail sector based on the information obtained from the purposively selected population.

## 4.11 Ethical considerations

This study uses human subjects; hence, the five fundamental ethical concerns of protection against harm, informed consent, anonymity and confidentiality, safety and respect, open, honest and trust and right to withdraw have been considered. The research project tasks were carried out after receiving ethical approval from the research ethics committee as well as the retail petroleum industry under study.

### 4.11.1 Informed consent

Festinger et al. (2023) asserts that Individuals have the right to be fully informed about the purpose, nature, benefits and risks associated with their participation in research. Researchers and professionals must seek informed consent from participants or clients prior to their involvement. This involves providing clear and understandable information and addressing any questions or concerns (Bianchi, 2022).

The aim and objectives of this study were communicated to all participants, and the data collection method was distributed to them prior to the data collection process. To ensure that respondents' identities are kept a secret, the researcher has delivered the consent form and requested that respondents fill it out. This research used a non-probability purposive sampling of convenience technique to select participants; however, participants were asked to participate voluntarily.

### 4.11.2 Anonymity and confidentiality

According to Olvera-Arellano (2022), individuals' identities and personal information should be kept confidential or anonymous to uphold and safeguard their right to privacy. It is important for researchers and professionals to establish protective measures to preserve the identity of participants or clients, maintaining that personal data is not disclosed without authorization.

The research's data sources were protected and kept private, and the participants' and company names have not been disclosed to unauthorised parties. As part of the study, anonymity and confidentiality were emphasised in briefings. Questionnaire responses and consent forms were safely stored, and only the researcher had access to them.

### 4.11.3 Safety and respect

Kraft et al. (2020) asserts that, in order to uphold the principles of safety and respect, it is crucial that individuals are treated with dignity, fairness, and consideration for their rights as well as their cultural values. Additionally, Kraft et al. (2020) states that, researchers and professionals should create a safe and respectful environment, considering the physical, cultural and emotional needs of their participants.

Participants were asked to participate voluntarily. No participant was pressured in any way to participate in the activities of the study. Challenging questions were simplified until participants understood the requirement/s so that participants could respond without feeling embarrassed.

### 4.11.4 Openness, Honesty and Trust

Transparency, honesty, and building a relationship of trust between professionals and participants are all necessary for ethical behavior. Being genuine about the nature

of the research or intervention and creating trust all help to foster ethical relationships and collaborations (Atkins, 2023).

Participants were informed that they would receive information about the study as needed. The research findings and presentation were conducted without manipulating or distorting data obtained from participants.

### 4.11.5 Right to withdraw

Individuals are entitled to withdraw from research or professional interventions at any time without harm. The right to withdraw should be clarified to participants or clients by researchers and professionals, ensuring that the withdrawal is voluntary and does not have any negative consequences for the participant (Pietilä et al., 2020).

Participants of this research study were made aware of their ability to leave the study at any time.

## 4.12 Chapter Summary

This chapter delineated the research procedures and the rationale for undertaking this study. The research adopts a positivist philosophical assumption, contributing to a comprehensive understanding of an IT security compliance and adoption awareness model.

A quantitative research design was selected, aligning with the survey approach that best serves the research's objectives. The chapter outlines the data collection methods, namely questionnaires and observations, and underscores the use of statistical data analysis, with SPSS as the chosen analytical tool. The participant selection process was described, emphasising purposive selection. The chapter also explains the data analysis method and discusses the measures taken to ensure the trustworthiness of the research.

These research methodologies, explained in this chapter, play a pivotal role in gaining insights into security compliance and adoption behaviours within the petroleum retail sector. They are instrumental in constructing an awareness model for the use of IT security policies.

# CHAPTER 5
# FINDINGS AND ANALYSIS

## 5.1 Introduction

This chapter serves as the core element of this research study, wherein thorough findings and analysis are conducted. This chapter describes the empirical findings and their implications and expands on the fundamental insights acquired via thoughtful data gathering and analysis. Answers to the research questions and objectives that are data-driven are investigated. Through an in-depth evaluation of these results, the study seeks to reveal recurring patterns, developments, and correlations that enhance an understanding of the topic being investigated.

The primary objective of this study is to develop an awareness model that encourages the use of information technology security policies within the petroleum retail industry. The study aims to derive valuable data from the questionnaires in order to provide practical insights and recommendations for improving cybersecurity practices and safeguarding important information inside the company.

The following research questions were formulated to guide the research:

SQ1: What IT security controls or policies are in place to protect organisational information? This research question focuses on exploring the existing IT security controls and policies implemented within the organisation to safeguard sensitive information. It seeks to identify the specific measures and protocols put in place to prevent unauthorised access and protect data from potential cyber threats.

SQ2: What organisational factors are used to promote IT security policy compliance and adoption? This research question examines the organisational factors that play a role in encouraging and promoting the adoption and adherence to IT security policies within the organisation. It aims to understand how the organisational culture, leadership support, training programs, and communication strategies contribute to enhancing cybersecurity awareness and compliance.

SQ3: What challenges are experienced with IT security compliance in the organisation? This research question addresses the potential obstacles and difficulties the organisation faces in achieving full IT security compliance. It seeks to identify the barriers, constraints,

or resistance that may hinder the effective implementation and enforcement of IT security policies and controls.

Through a comprehensive investigation of these research questions, the study intended to gain valuable insights into the current state of IT security practices and the contributing organisational factors and challenges. The findings have provided practical recommendations and strategies for strengthening IT security measures and ensuring better compliance within the organisation, thereby enhancing the overall cybersecurity posture.

## 5.2 Access management

Access management, often known as identity and access management (IAM), is a security and IT management practice that focuses on controlling and monitoring the access granted to individuals and systems for resources and data within an organisation's IT environment. The main objective of access management is to guarantee that authorised individuals or systems possess a suitable level of access to the correct resources, while unauthorised or excessive access is limited or refused (Gopal & Haran, 2020).

**Report**

| Ward Method | | The password policy is available and easily accessible to me. | I frequently utilize a Virtual Private Network (VPN) in my day-to-day activities. | I have the capability to use my personal computer to gain access to organizational data and applications. | I have the capability to use my work computer to access personal data and applications. | I use my personal device to access organizational sensitive or personal information (POPIA / confidential). | Occasionally, I use public spaces (airplane/airport, hotel, restaurant) to access confidential data or information while traveling or working remotely. | Occasionally, I connect to public Wi-Fi (airport, hotel, restaurant) to access confidential data or information while traveling or working remotely. | The computer provided by my organization grants me access to various social media platforms. |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Mean | 4.57 | 4.71 | 1.29 | 1.86 | 3.71 | 1.71 | 2.00 | 3.14 |
| | N | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 |
| | Std. Deviation | .535 | .756 | .488 | .900 | .756 | .488 | .816 | 1.069 |
| 2 | Mean | 4.64 | 4.18 | 1.91 | 1.91 | 4.00 | 3.91 | 3.82 | 3.55 |
| | N | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 |
| | Std. Deviation | .505 | .982 | .701 | .701 | .447 | .302 | .405 | .522 |
| 3 | Mean | 4.56 | 4.68 | 3.88 | 3.00 | 3.92 | 4.00 | 3.92 | 3.16 |
| | N | 25 | 25 | 25 | 25 | 25 | 25 | 25 | 25 |
| | Std. Deviation | .583 | .476 | .526 | .913 | .277 | .000 | .277 | .898 |
| 4 | Mean | 4.62 | 4.00 | 3.77 | 3.00 | 3.62 | 2.54 | 2.69 | 3.23 |
| | N | 13 | 13 | 13 | 13 | 13 | 13 | 13 | 13 |
| | Std. Deviation | .506 | .816 | .725 | 1.000 | .506 | .519 | .630 | .439 |
| 5 | Mean | 4.36 | 5.00 | 2.27 | 2.73 | 2.09 | 3.36 | 2.91 | 3.55 |
| | N | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 |
| | Std. Deviation | .809 | .000 | 1.104 | 1.104 | .944 | .674 | .944 | .934 |
| Total | Mean | 4.55 | 4.52 | 3.00 | 2.66 | 3.55 | 3.36 | 3.30 | 3.30 |
| | N | 67 | 67 | 67 | 67 | 67 | 67 | 67 | 67 |
| | Std. Deviation | .585 | .725 | 1.219 | 1.023 | .858 | .883 | .888 | .798 |

*Figure 5.1 Cluster Analysis*

A cluster analysis, as presented in Figure 5.1 above, was performed with the objective of revealing behavioural patterns among employees in relation to their access to organisational resources, as well as identifying strategies to improve adherence to security standards. Based on the available evidence, it is possible to derive the following interpretation:

**Compliance Variation**

Substantial disparities exist in the adherence to access management techniques among distinct groups of personnel. Certain clusters, such as Cluster 1, appear to adhere more strictly to established best practices, whereas clusters 2 and 5 demonstrate a more varied and less consistent adherence. The observed adherence could be attributed to coordinated access management protocols, which could be by using passcodes with an uncompromised digital footprint. In contrast, the lack of strict adherence observed in

clusters 2 and 5 suggests that access management lacks security measures that can safeguard IT infrastructures and protect access to sensitive information. In essence, the lack of standardised or coordinated protocols exposes the vulnerability of IT systems to threats (internal and external).

In the study conducted by Rawal, Gunasekaran Manogaran and Peter (2023), it was stated that access management constitutes one of the most important safeguarding measures to eliminate potential cybersecurity threats. Therefore, access management is an essential factor to consider regarding cybersecurity.

***1. Personal Device Usage***

The inconsistency presented in Figure 5.1 in the manner in which employees utilise personal devices to access organisational data is evident, with notable differences among different clusters of employees. Some clusters show disagreement, while others display agreement or neutrality on this matter.

This variation in attitudes and practices concerning the use of personal devices for accessing organisational data could be indicative of the model of cybersecurity adopted by the organization/s targeted for this study. In addition, the variation in the inconsistency could be attributed to a well-defined policy or approach in place to address this issue effectively. This lack of consistency could potentially lead to security vulnerabilities and data breaches, as different clusters of employees may adopt varying levels of security measures when accessing sensitive information on personal devices.

To address this inconsistency and enhance the organisation's cybersecurity stance, it is crucial to conduct a comprehensive review of the existing IT security policies. The research findings can serve as a starting point for identifying areas that require improvement and further refinement.

Additionally, targeted training and awareness programs should be implemented to educate employees about the importance of secure practices when accessing organisational data on personal devices. Ensuring all employees are well-informed about the organisation's IT security policies and best practices can help establish a unified approach to data access and minimise potential risks.

Furthermore, IT security managers and organisational leaders should collaborate to develop clear and consistent guidelines regarding the use of personal devices for work-related tasks. By establishing a standardised policy and providing the necessary resources and tools for secure access, the organisation can create a more cohesive and secure environment for data handling.

***2. Public Spaces and Wi-Fi Usage***

The findings that some clusters indicate frequent use of public spaces and Wi-Fi to access confidential information can be considered as a high-level exposure of a significant security risk for the organisation. This is because accessing sensitive data in public spaces and over public Wi-Fi networks increases the vulnerability of the information to potential cyber threats and unauthorised access. Public spaces, such as coffee shops, airports, and hotels, often have open and unsecured Wi-Fi networks, making them easy targets for cybercriminals to intercept data transmissions. These networks lack the encryption and security measures present in private and secure corporate networks, leaving data susceptible to eavesdropping and unauthorised access.

To address this security risk, the organisation must take immediate and proactive measures:

a. **Raise Awareness:** Conduct targeted cybersecurity awareness training for all employees, emphasising the risks associated with accessing confidential information in public spaces and over public Wi-Fi networks. Employees need to be aware of the potential consequences and the importance of adhering to security best practices.
b. **Develop Mobile Device Policies:** Establish clear and comprehensive mobile device policies that outline the permitted and prohibited activities when accessing organisational data on personal devices. Encourage the use of company-approved security apps and tools to enhance the protection of sensitive information.
c. **Secure Wi-Fi Connections:** Implement security measures for employees who need to access company data while on the move. Encourage the use of secure personal hotspot connections or portable Wi-Fi routers to ensure a safe and private connection.

d. **Monitor and Enforce Policy Compliance:** Regularly monitor employees' adherence to the established security policies and take appropriate action against breaches or non-compliance. Consistent enforcement of security measures creates a culture of accountability and reinforces the importance of data protection.
e. **Regular Security Audits:** Conduct regular security audits and risk assessments to identify potential vulnerabilities and areas of improvement. Address any identified weaknesses promptly to enhance the organisation's overall cybersecurity posture.

The organisation can significantly reduce the risk of data breaches and unauthorised access by addressing the issue of accessing confidential information in public spaces and over public Wi-Fi networks. With a proactive approach to cybersecurity and a commitment to educating employees about best practices, the organisation can create a secure and resilient environment for handling sensitive information.

### *3. Work Computer for Personal Access*

The variation in how employees use work computers for personal access poses a significant concern for the organisation's cybersecurity. Allowing personal access to work computers can potentially expose sensitive organisational data to unnecessary risks and security vulnerabilities.

There is a need to develop and communicate clear policies and guidelines regarding the use of work computers for personal access. In this case, it should be mandatory that employees are duly informed about the permissible usage and prohibited usage of office electronic devices such as laptops, thus ensuring that they understand the potential risks of using work devices for personal purposes.

In order to mitigate this security risk, the organisation must take immediate and proactive measures to address it:

a. **Tailored Training and Awareness**: Targeted cybersecurity training can be developed to address the specific behaviours and needs identified in each cluster. For example, employees in Cluster 2 might benefit from additional

training on the risks associated with using public Wi-Fi. Empower employees to recognise potential threats and understand their responsibilities in safeguarding organisational data.

b. **Policy Accessibility and Understanding**: High agreement on the accessibility of password policies indicates that employees are aware of the policies but may need more guidance, refresher or incentives to follow them consistently.
c. **Monitoring, Auditing and Feedback**: Regular monitoring and audit of work computers to identify any unauthorised or risky personal activities. Feedback on access management practices can reinforce positive behaviours and correct non-compliance.
d. **Network Segmentation**: Employ network segmentation to isolate personal activities from the organisation's critical systems and data. This practice ensures that personal access does not compromise the security of sensitive information.
e. **Enforce Consequences**: Clearly communicate the consequences of violating the policies related to personal access on work computers. Consistent enforcement of policies can deter employees from engaging in risky behaviours.
f. **Encourage Personal Device Policies**: Encourage employees to use personal devices, such as smartphones or tablets, for personal activities instead of using work computers. This helps maintain the integrity and security of work devices solely for work-related tasks.

The identified clusters, such as with varying access practices, underscore the need for tailored interventions. Although one-size-fits-all approaches may not be effective, it is important to ensure that a series of processes are instituted such that targeted measures that will mitigate potential compromise of cybersecurity threats are eliminated. In addition, an implementation strategy such as customisation access, expiration of access, and systematic renewal of access is developed and enforced. The organisation can promote secure data access and minimise potential risks by customising interventions.

A holistic approach through periodic upgrades of security measures to cybersecurity is essential to foster a culture of security awareness and compliance throughout the organisation. This approach involves not only technical measures but also educating employees about cybersecurity best practices and emphasising their role in protecting sensitive data. By aligning all employees with organisational policies and practices, the organisation can create a unified front in safeguarding data and mitigating potential threats. Employees play a vital role as the first line of defence, and their understanding and adherence to access management policies are critical in maintaining a robust cybersecurity posture.

In summary, the cluster analysis serves as a foundation for strengthening the organisation's access management practices. Tailored interventions, continuous monitoring, and a holistic approach to cybersecurity are fundamental to ensure a secure and resilient environment for data access and management.

## 5.3 Knowledge

**Error! Reference source not found.** and **Error! Reference source not found.** shows the usage and correlation of VPN usage and access to training.

**VPN is easy to use, in my opinion.**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | I don't know | 1 | 1.5 | 1.5 | 1.5 |
| | Disagree | 2 | 3.0 | 3.0 | 4.5 |
| | Agree | 18 | 26.9 | 26.9 | 31.3 |
| | Strongly agree | 46 | 68.7 | 68.7 | 100.0 |
| | Total | 67 | 100.0 | 100.0 | |

*Figure 5.2 VPN Usage*

**Correlations**

| | | VPN is easy to use, in my opinion. | Within my organization, I have access to a training platform that offers cybersecurity-related training topics. |
|---|---|---|---|
| VPN is easy to use, in my opinion. | Pearson Correlation | 1 | .203 |
| | Sig. (2-tailed) | | .100 |
| | N | 67 | 67 |
| Within my organization, I have access to a training platform that offers cybersecurity-related training topics. | Pearson Correlation | .203 | 1 |
| | Sig. (2-tailed) | .100 | |
| | N | 67 | 67 |

*Figure 5.3 Correlations between the Use of VPN and access to training*

### *1. Use of VPN and access to training*

The majority of respondents find VPN (Virtual Private Network) easy to use, which is a positive indication of the effectiveness of the organisation's VPN implementation and user experience. It suggests employees have had a smooth and hassle-free experience while using the VPN to access organisational resources remotely.

The correlation coefficient of 0.203 and the p-value (Sig.) of 0.100 suggest a weak positive correlation between the perception that a VPN is easy to use and access to a training platform that offers cybersecurity-related training topics. A correlation coefficient of 0.203 indicates a positive relationship between the two variables (perception of VPN ease of use and access to cybersecurity training). However, the value being close to zero suggests that the correlation is weak, meaning that the strength of the relationship is not substantial.

The p-value of 0.100 indicates the statistical significance of the correlation. In hypothesis testing, a p-value below a certain significance level (often set at 0.05) suggests that the correlation is statistically significant, meaning that the relationship observed is unlikely to occur by chance. However, in this case, the p-value is above the commonly used

significance level of 0.05, indicating that the correlation is not statistically significant at the 5% level. Therefore, it is hard to conclude that there is a strong relationship between these two variables.

Based on the correlation coefficient and p-value, it can be concluded that there is a weak positive correlation between the perception that a VPN is easy to use and access to a training platform with cybersecurity-related training topics. However, this correlation is not statistically significant, suggesting that the observed relationship could have occurred by chance. Further research with a larger sample size or different variables may be needed to determine if there is a significant and stronger relationship between these two factors.

Based on the overall positive perception of VPN usage ease, it is essential for the organisation to continue providing support and possibly highlight the VPN as a valuable tool in its cybersecurity policy. Emphasising the VPN's ease of use and its role in enhancing remote access security can further encourage employees to utilise this important security measure. Clear communication about its benefits and user-friendly features can reinforce its importance as a key component of the organisation's cybersecurity strategy.

Regarding the lack of a significant relationship between training access and the perception of VPN ease of use, it is crucial for the organisation to evaluate the content and delivery of cybersecurity training. Understanding user needs and actual tool usage is essential to ensure that the training aligns with employees' requirements and effectively enhances their understanding and confidence in using cybersecurity tools like VPNs.

**Error! Reference source not found.** below illustrates the level of understanding regarding cybersecurity policies and awareness at the workplace

**In terms of cybersecurity policies and awareness, what is your level of understanding?**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Understand fully | 34 | 50.7 | 50.7 | 50.7 |
| | Understand | 29 | 43.3 | 43.3 | 94.0 |
| | Neutral | 4 | 6.0 | 6.0 | 100.0 |
| | Total | 67 | 100.0 | 100.0 | |

*Figure 5.4 Cybersecurity Policy Awareness*

The data as presented above indicate that the majority have a positive understanding of cybersecurity policies and awareness.

**I understand my responsibility / obligation to log all security related incidents.**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Disagree | 2 | 3.0 | 3.0 | 3.0 |
| | Agree | 25 | 37.3 | 37.3 | 40.3 |
| | Strongly agree | 40 | 59.7 | 59.7 | 100.0 |
| | Total | 67 | 100.0 | 100.0 | |

*Figure 5.5 Obligation to log incidents*

There seems to be a consensus about understanding this responsibility.

**I understand what is expected of me from the cybersecurity perspective.**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Disagree | 2 | 3.0 | 3.0 | 3.0 |
| | Agree | 21 | 31.3 | 31.3 | 34.3 |
| | Strongly agree | 44 | 65.7 | 65.7 | 100.0 |
| | Total | 67 | 100.0 | 100.0 | |

*Figure 5.6 Cybersecurity Expectations*

This shows a strong alignment with cybersecurity expectations.

**I know where to find information about cybersecurity.**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | I don't know | 2 | 3.0 | 3.0 | 3.0 |
| | Disagree | 3 | 4.5 | 4.5 | 7.5 |
| | Agree | 29 | 43.3 | 43.3 | 50.7 |
| | Strongly agree | 33 | 49.3 | 49.3 | 100.0 |
| | Total | 67 | 100.0 | 100.0 | |

*Figure 5.7 Information about cybersecurity*

**I know where to report cybersecurity related questions.**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | I don't know | 1 | 1.5 | 1.5 | 1.5 |
| | Disagree | 2 | 3.0 | 3.0 | 4.5 |
| | Agree | 30 | 44.8 | 44.8 | 49.3 |
| | Strongly agree | 34 | 50.7 | 50.7 | 100.0 |
| | Total | 67 | 100.0 | 100.0 | |

*Figure 5.8 Reporting cybersecurity questions*

The high percentage of respondents who agree or strongly agree that they know where to find information about cybersecurity (92.6%) and where to report questions (95.5%) indicates a positive perception of access to cybersecurity resources and reporting channels within the organisation.

## 5.4 Security

**Error! Reference source not found.** below shows the analysis of responses to the question regarding attempted attacks against work computers.

**Cybercriminals or scammers have previously attempted to carry out a cyberattack against my work computer.**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | I don't know | 6 | 9.0 | 9.0 | 9.0 |
| | Strongly disagree | 13 | 19.4 | 19.4 | 28.4 |
| | Disagree | 17 | 25.4 | 25.4 | 53.7 |
| | Agree | 20 | 29.9 | 29.9 | 83.6 |
| | Strongly agree | 11 | 16.4 | 16.4 | 100.0 |
| | Total | 67 | 100.0 | 100.0 | |

*Figure 5.9 Previous cyberattacks*

**Majority without Experience:** By merging the "Strongly disagree" and "Disagree" categories, it is observed that 44.8% of the participants have not encountered any hack attempts on their work computers.

**Significant Experience with Attacks:** A substantial proportion, specifically 46.3% (comprising respondents who indicated agreement or strong agreement), have reported experiencing an attack.

**Uncertainty Exists:** The proportion of respondents, amounting to 9.0%, who selected the response option "I don't know" could potentially suggest a deficiency in their

awareness or comprehension regarding the definition as well as the features of a cyberattack. Alternatively, it is possible that these individuals may lack the necessary resources or expertise to identify and discern an attempted cyberattack.

Further investigation is necessary in order to have a comprehensive understanding of the profiles or features of those who have been subjected to attacks as compared to those who have not.

**Education and Training:** The presented responses may suggest a requirement for educational or training interventions aimed at enhancing the ability to identify and effectively manage cyberattack efforts.

**Security Measures Assessment:** To comprehend the reasons behind the occurrence of attack attempts experienced by about 50% of the respondents, it is important to conduct an evaluation of the current security measures and procedures used inside the organisation.

**Error! Reference source not found.** below shows the correlations between previous attempts and home network/Wi-Fi.

**Correlations**

| | | Cybercriminals or scammers have previously attempted to carry out a cyberattack against my work computer. | I understand security capabilities around my home network / Wi-Fi. |
|---|---|---|---|
| Cybercriminals or scammers have previously attempted to carry out a cyberattack against my work computer. | Pearson Correlation | 1 | .007 |
| | Sig. (2-tailed) | | .958 |
| | N | 67 | 67 |
| I understand security capabilities around my home network / Wi-Fi. | Pearson Correlation | .007 | 1 |
| | Sig. (2-tailed) | .958 | |
| | N | 67 | 67 |

*Figure 5.10 Correlations on previous attempts vs home network/Wi-Fi*

**Error! Reference source not found.** below shows the correlations between previous attempts and cybersecurity expectations.

**Correlations**

| | | Cybercriminals or scammers have previously attempted to carry out a cyberattack against my work computer. | I understand what is expected of me from the cybersecurity perspective. |
|---|---|---|---|
| Cybercriminals or scammers have previously attempted to carry out a cyberattack against my work computer. | Pearson Correlation | 1 | .008 |
| | Sig. (2-tailed) | | .950 |
| | N | 67 | 67 |
| I understand what is expected of me from the cybersecurity perspective. | Pearson Correlation | .008 | 1 |
| | Sig. (2-tailed) | .950 | |
| | N | 67 | 67 |

*Figure 5.11 Correlations on previous attempts vs cybersecurity expectations*

The findings suggest a lack of significant connection between the variables under investigation. The Pearson correlation coefficients have values of .007 and .008, indicating a proximity to zero. This observation implies that there is no direct correlation between one's comprehension of security measures pertaining to their home network and their likelihood of encountering a cyberattack on their work computer. Likewise, no discernible association exists between comprehending the anticipated requirements in the realm of cybersecurity and encountering a cyberattack.

The p-values (Sig. (2-tailed)) of .958 and .950 are far greater than the typical significance level of 0.05, indicating that these correlations lack statistical significance. In alternative terms, it is possible that any apparent correlation may be attributed to random occurrences.

**Understanding Security Capabilities**: There is a lack of empirical data supporting the notion that understanding security capabilities around a home network/Wi-Fi has any bearing on whether a person has experienced a cyberattack on their work computer.

**Understanding Cybersecurity Expectations**: There is no empirical data to suggest that understanding what is expected from a cybersecurity perspective has any correlation with experiencing a cyberattack.

**Potential Actions**: Given the lack of correlation, it may be valuable to investigate other factors that could be influencing the likelihood of a cyberattack. Perhaps the nature of the work, the type of organisation, the tools used, or the training provided might be more relevant.

The lack of correlation does not imply that these factors are not critical in the field of cybersecurity; rather, it suggests that they may not be directly linked with the occurrence of cyberattacks within the specific dataset under consideration.

## 5.5 Training

**Error! Reference source not found.** below shows the results of the frequency at which the organisation provides cybersecurity training.

**What is the frequency at which your organization provides cybersecurity training?**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Yearly | 25 | 37.3 | 37.3 | 37.3 |
| | Quarterly | 35 | 52.2 | 52.2 | 89.6 |
| | Monthly | 7 | 10.4 | 10.4 | 100.0 |
| | Total | 67 | 100.0 | 100.0 | |

*Figure 5.12 Training frequency*

**Most Frequent Training - Quarterly:** A majority of the participants (52.2%) indicated that their respective organisations offer cybersecurity training on a quarterly basis.

**Yearly Training:** A notable proportion, specifically 37.3%, indicated that the training is administered annually.

**Least Frequent - Monthly:** A smaller proportion, comprising 10.4%, reported that the training is conducted monthly.

**Positive emphasis on regular training:** The findings reveal that a significant proportion (89.6%) of participants undergo regular cybersecurity training, either on a quarterly or yearly basis. This observation suggests that organisations have a strong dedication to ensuring that their workforce is well-informed and knowledgeable about cybersecurity issues.

**Potential for more frequent training:** Organisations that offer annual training programs may consider exploring the possibility of enhancing the frequency of these initiatives, particularly in light of the dynamic nature of cybersecurity threats and evolving best practices.

**Consideration of training needs and content:** The optimal frequency of training may differ based on the specific roles, responsibilities, and prevailing security landscape. Roles with larger security obligations may require more frequent training, whereas less frequent, high-level updates may be suitable for roles with lower security responsibilities.

a. **Exploration of monthly training:** It would be of academic interest to investigate the factors contributing to the lower proportion of responders engaging in monthly training and whether this pattern aligns with particular jobs or responsibilities within the business.
b. **Tailored training plans:** It is recommended to consider developing customised training programs specifically designed to align with job roles and responsibilities and unique cybersecurity risks and issues encountered by various segments inside the organisation.
c. **Training effectiveness evaluation:** Assess the effectiveness of the current training frequency and topics in order to ascertain its alignment with the objectives and requirements of the organisation.
d. **Engagement with employees:** Engage with employees to gain insights into their perspectives and requirements pertaining to the frequency and content of

training. The contribution of individuals can be of great value in the development of a training program that is both efficient and engaging.

Overall, the data indicates a favourable pattern in the organisation's dedication to cybersecurity training, exhibiting diverse frequencies that might be further customised to address unique requirements and objectives.

**Error! Reference source not found.** below shows the results of participation in online or in-person cybersecurity training sessions.

**Within the past six months, I have participated in online or in-person training sessions that focused on cybersecurity.**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Disagree | 5 | 7.5 | 7.5 | 7.5 |
| | Agree | 27 | 40.3 | 40.3 | 47.8 |
| | Strongly agree | 35 | 52.2 | 52.2 | 100.0 |
| | Total | 67 | 100.0 | 100.0 | |

*Figure 5.13 Participation in Cybersecurity Training Sessions*

**High Participation:** A total of 92.5% of respondents indicated their agreement or strong agreement with having engaged in cybersecurity training sessions within the preceding six-month period.

**Low Non-Participation:** Only 7.5% of respondents express disagreement, suggesting a lack of recent engagement in training activities.

Figure 5.16 below shows the results of employee access to a training platform for cybersecurity-related topics.

**Within my organization, I have access to a training platform that offers cybersecurity-related training topics.**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Strongly disagree | 1 | 1.5 | 1.5 | 1.5 |
| | Disagree | 1 | 1.5 | 1.5 | 3.0 |
| | Agree | 17 | 25.4 | 25.4 | 28.4 |
| | Strongly agree | 48 | 71.6 | 71.6 | 100.0 |
| | Total | 67 | 100.0 | 100.0 | |

*Figure 5.14 Access to training platform for cybersecurity topics*

**High Availability:** A substantial percentage (96.0%) of the participants indicated that they possess access to a training platform within their respective organisations, which provides them with cybersecurity-related training topics.

**Minimal Dissent:** A mere 3.0% of individuals (Strongly Disagree + Disagree) either lack access or express disagreement with the statement.

**Strong Training Culture:** The organisation has a notable prioritisation of cybersecurity training, as seen by its extensive accessibility and substantial rates of engagement.

**Opportunity for Continued Education:** Despite the presence of extensive access and active engagement, there remains a need for ongoing or improved training initiatives, particularly aimed at the minority segment that has exhibited limited recent participation.

**Investigate Dissent:** It may be advantageous to investigate the reasons behind the limited accessibility of the training platform for a minority of individuals, as well as the factors contributing to the lack of recent participation in training among certain individuals.

**Assessment of Training Quality:** Given the substantial level of involvement and accessibility, it would be of considerable importance to assess the effectiveness and satisfaction associated with the training provided.

**Targeted Training Programs:** Develop or improve training programs to guarantee their alignment with the organisation's present cybersecurity requirements and complexities.

**Regular Training Updates:** To maintain a consistent and adaptive approach to the evolving cybersecurity landscape, it is essential to establish a structured schedule for regular training updates. This will facilitate ongoing learning and enable individuals to stay informed of the latest developments in the field.

The data presented provides a favourable perspective on the organisation's cybersecurity training, which may serve as a catalyst for ongoing emphasis and advancement in this critical domain.

## 5.6 Data Sharing

**Error! Reference source not found.** below shows the percentage of how often employees share organisational information or data with external parties.

**I regularly share organisational information or data with partners, contractors, customers, suppliers, or vendors.**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | I don't know | 1 | 1.5 | 1.5 | 1.5 |
| | Strongly disagree | 8 | 11.9 | 11.9 | 13.4 |
| | Disagree | 17 | 25.4 | 25.4 | 38.8 |
| | Agree | 41 | 61.2 | 61.2 | 100.0 |
| | Total | 67 | 100.0 | 100.0 | |

*Figure 5.15 Data Sharing with external parties*

A majority of respondents, specifically 61.2%, express agreement with the practice of frequently sharing organisational information or data with various external entities such as partners, contractors, customers, suppliers, or vendors.

**Error! Reference source not found.** below shows the percentage of how often employees utilise social media platforms to share organisational information or data.

**I utilize social media platforms, including WhatsApp, Telegram, Facebook, and Instagram, as channels for sharing organizational data.**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Strongly disagree | 1 | 1.5 | 1.5 | 1.5 |
| | Disagree | 10 | 14.9 | 14.9 | 16.4 |
| | Agree | 56 | 83.6 | 83.6 | 100.0 |
| | Total | 67 | 100.0 | 100.0 | |

*Figure 5.16 Data Sharing via social media*

A substantial proportion (83.6%) of respondents acknowledge their utilisation of various social media platforms, such as WhatsApp, Telegram, Facebook, and Instagram, for the purpose of sharing corporate data.

**Error! Reference source not found.** below shows the correlations between sharing data via social media platforms and sharing data with external parties.

**Correlations**

| | | I utilize social media platforms, including WhatsApp, Telegram, Facebook, and Instagram, as channels for sharing organizational data. | I regularly share organisational information or data with partners, contractors, customers, suppliers, or vendors. |
|---|---|---|---|
| I utilize social media platforms, including WhatsApp, Telegram, Facebook, and Instagram, as channels for sharing organizational data. | Pearson Correlation | 1 | -.068 |
| | Sig. (2-tailed) | | .587 |
| | N | 67 | 67 |
| I regularly share organisational information or data with partners, contractors, customers, suppliers, or vendors. | Pearson Correlation | -.068 | 1 |
| | Sig. (2-tailed) | .587 | |
| | N | 67 | 67 |

*Figure 5.17 Correlations on sharing data via social media and with external parties*

The study examines the correlation between the utilisation of social media platforms and the practice of sharing content with external parties. The analysis reveals a Pearson correlation coefficient of -0.068, indicating a weak negative relationship. The corresponding p-value of 0.587 suggests that this correlation is not statistically significant ($p > 0.05$), indicating that the correlation could be due to random chance.

The investigation demonstrates that a considerable percentage of employees engage in the utilisation of social media platforms for the purpose of sharing organisational data. Additionally, a substantial number of employees consistently engage in the sharing of information with diverse external entities. The absence of a substantial association between these two behaviours implies that they could be affected by distinct variables or motivations.

The aforementioned findings prompt critical inquiries regarding data security and organisational compliance. The extensive utilisation of social media platforms for the purpose of sharing corporate data carries inherent dangers that demand the establishment of explicit standards, provision of training, and implementation of technical steps to assure the adoption of secure practices. The act of regularly sharing information with external parties necessitates careful examination to verify that it is in accordance with the policies and legal obligations of the organisation.

## 5.7 Compliance

**Error! Reference source not found.** below shows the percentage of how often employees utilise social media platforms to share organisational information or data.

**My work computer has been successfully hacked or exploited in the past.**

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|
| Agree | 1 | 1.5 | 1.5 | 1.5 |
| Disagree | 16 | 23.9 | 23.9 | 26.9 |
| I don’t know | 2 | 3.0 | 3 | 100 |
| Strongly agree | 1 | 1.5 | 1.5 | 3 |
| Strongly disagree | 47 | 70.1 | 70.1 | 97 |
| Total | 67 | 100.0 | 100.0 | |

*Figure 5.18 Hacking or exploits*

**Agree:** The data indicates that a significant majority of respondents, specifically 70.1%, expressed strong disagreement, suggesting that most individuals hold the belief that their work computer has not been subjected to effective hacking or exploitation.

**Strongly Agree:** A total of 3.0% of respondents expressed strong agreement with the statement that their work computer has been successfully targeted by hacking or exploitation techniques.

**Majority's perception:** The fact that 94% of respondents agree (including "Strongly Disagree") that their work computers have not been successfully hacked or exploited is

a positive indication. This suggests that the majority of employees feel confident in the effectiveness of the organisation's cybersecurity measures. Their perception aligns with the idea that the organisation's security measures are working as intended and that there is a lower likelihood of successful hacking attempts.

**Small percentage reporting successful hacks:** 3.0% of respondents reported that their work computers had been successfully hacked or exploited; this indicates that there have been some instances of successful breaches. While the percentage is relatively small, it is still important for the organisation to investigate these cases and understand the nature of the breaches, impact and potential patterns. This can help identify potential vulnerabilities and guide improvement in cybersecurity measures.

**Uncertainty About Hacks:** 3.0% of respondents do not know whether their machines have been previously hacked or not; this could indicate a lack of awareness about potential security breaches. It is essential for the organisation to educate its employees about the signs of hacking attempts and how to report any suspicious activities.

Overall, the positive perception of the majority regarding the security of their work computers is a good sign. However, it is important to note that cybersecurity is an ongoing effort. Even with a high percentage of respondents feeling secure, the organisation should continue to monitor and update its cybersecurity measures to stay ahead of evolving threats while ensuring employees are educated about cybersecurity best practices.

**Error! Reference source not found.** below shows the percentage of employees who utilise the available phishing platforms to report suspected email phish.

**What do you do if you suspect an email has been phished or if you spot any non-compliance concerns?**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Report to line manager | 5 | 7.5 | 7.7 | 7.7 |
| | Report to service desk | 5 | 7.5 | 7.7 | 15.4 |
| | Report via phish alert | 55 | 82.1 | 84.6 | 100.0 |
| | Total | 65 | 97.0 | 100.0 | |
| Missing | System | 2 | 3.0 | | |
| Total | | 67 | 100.0 | | |

*Figure 5.19 Non-compliance actions*

The findings of the report indicate that a substantial proportion, specifically 84.6%, of the participants expressed their intention to report suspicious emails or messages through the utilisation of a phish alert system.

A significant proportion of participants express a preference for utilising a dedicated phish alert method to report instances of potential phishing or non-compliance. This indicates a well-adopted practice and suggests that the organisation's alert system is not only well-built but also highly regarded by employees. This positive perception speaks to the effectiveness of the system in addressing security concerns and potential threats.

While the dedicated phish alert method is well-received, providing additional channels for reporting can enhance overall incident reporting and response capabilities. It can also accommodate the preferences of those who might not find the dedicated method suitable for their situation. The organisation can better cater to different communication preferences by diversifying reporting outlets. This might involve options like service desk, report to line management, direct messaging, phone calls, or even in-person reporting. Ensuring that employees are aware of these alternative methods and promoting their use can help create a culture of active reporting and incident response.

## Clustering Analysis

**Error! Reference source not found.** below depicts a clustering analysis of the various questions that were asked to respondents.

**Report**

| Ward Method | | ID | I understand what is expected of me from the cybersecurity perspective. | I know where to find information about cybersecurity. | I know where to report cybersecurity related questions. | I understand my responsibility / obligation to log all security related incidents. | In terms of cybersecurity policies and awareness, what is your level of understanding?Required to answer. Likert. |
|---|---|---|---|---|---|---|---|
| 1 | Mean | 26.93 | 4.64 | 4.29 | 4.14 | 4.79 | 1.29 |
| | N | 14 | 14 | 14 | 14 | 14 | 14 |
| | Std. Deviation | 21.131 | .497 | .469 | .363 | .426 | .469 |
| 2 | Mean | 33.21 | 4.11 | 3.89 | 3.89 | 3.89 | 2.16 |
| | N | 19 | 19 | 19 | 19 | 19 | 19 |
| | Std. Deviation | 21.635 | .459 | .459 | .315 | .315 | .375 |
| 3 | Mean | 38.83 | 5.00 | 5.00 | 5.00 | 5.00 | 1.00 |
| | N | 23 | 23 | 23 | 23 | 23 | 23 |
| | Std. Deviation | 18.463 | .000 | .000 | .000 | .000 | .000 |
| 4 | Mean | 15.00 | 3.50 | 1.00 | 2.50 | 4.50 | 2.50 |
| | N | 2 | 2 | 2 | 2 | 2 | 2 |
| | Std. Deviation | 4.243 | .707 | .000 | 2.121 | .707 | .707 |
| 5 | Mean | 38.56 | 5.00 | 4.56 | 5.00 | 4.56 | 1.89 |
| | N | 9 | 9 | 9 | 9 | 9 | 9 |
| | Std. Deviation | 12.012 | .000 | .527 | .000 | .527 | .333 |
| Total | Mean | 34.00 | 4.63 | 4.36 | 4.43 | 4.57 | 1.55 |
| | N | 67 | 67 | 67 | 67 | 67 | 67 |
| | Std. Deviation | 19.485 | .546 | .829 | .701 | .557 | .610 |

*Figure 5.20 Clustering Analysis*

**Cluster 1:**

- The participants had a high average score in their comprehension of expectations, ability to find relevant information, and sense of responsibility in logging incidents.
- The group demonstrates a strong level of awareness and competence in the field of cybersecurity.

**Cluster 2:**

- Cluster 2 exhibits a marginally diminished level of understanding and awareness compared to Cluster 1; however, it remains higher than the norm.
- This group might benefit from targeted training or information sessions.

**Cluster 3:**

- Perfect mean score of 5 on the majority of variables.
- This could represent the experts or most informed individuals in the sample.

**Cluster 4:**

- The smallest cluster with varied responses, including a low score on knowing where to find information.
- This particular group may necessitate further focused educational interventions or access to supplementary resources.

**Cluster 5:**

- Comparable to Cluster 3 in many respects, but with a slightly different emphasis on knowing where to find information.
- Likely also highly informed and engaged.

The overall data indicates a high level of understanding and awareness regarding cybersecurity policies and practices among the participants.

The clustering identifies specific groups that may require different approaches or levels of support:

- For clusters showing a strong understanding (e.g., Clusters 1, 3, and 5), continue to foster this awareness and possibly engage them in peer-to-peer support or advocacy.
- To further cultivate clusters demonstrating a high level of understanding, such as Clusters 1, 3, and 5, it is recommended to sustain this awareness and

maybe involve them in activities that promote peer-to-peer support or engagement.

- Clusters that demonstrate lower levels of understanding or awareness, such as Cluster 2, may benefit from specialised training or the provision of resources aimed at improving their knowledge and alignment with cybersecurity objectives.
- Cluster 4, characterised by its relatively modest size and diverse nature, may necessitate individualised attention to evaluate unique requirements and offer suitable assistance effectively.

A thorough understanding of these patterns and clusters can provide valuable insights for developing a focused approach to strengthening an organisation's cybersecurity awareness, education, and compliance. This approach should account for the diverse degrees of knowledge and requirements across different groups.

## 5.8 Chapter Summary

The findings in this chapter reveal that employees in an organisation lack access to IT security policies, leading to potential data theft and system compromise. Some employees lack the necessary expertise to identify and differentiate cyberattacks, resulting in uncertainty about potential exploits. Training and education programs can help develop a security culture and alert employees to potential hazards. Employees can access work data from personal devices, which lack the same security measures as organisational devices, posing a cybersecurity risk.

The extensive use of social media platforms for sharing corporate data also raises significant security concerns, as it allows employees to share confidential information with anyone, potentially leading to data breaches and leaks.

Organisations should review their security policies to ensure they align with current best practices and to ensure that standardised policies, along with necessary resources and tools for secure access, can create a cohesive and secure environment for data handling. Addressing issues related to accessing and sharing confidential information thus reduces the risk of data breaches and unauthorised access.

The research findings highlight a positive and high level of awareness and understanding among employees regarding the importance of strong passwords in enhancing cybersecurity. Employees are well informed about the risks associated with weak passwords and the significance of adhering to best practices. Findings present a positive response to authentication apps and SMS codes, suggesting that employees are receptive to these technological advancements in cybersecurity. They appreciate the convenience and ease of these methods and tools.

# CHAPTER 6
# DISCUSSION, CONCLUSION AND RECOMMENDATIONS

## 6.1 Introduction

This chapter provides an in-depth summary of the results obtained from an extensive review of the relevant literature as well as the gathering and examination of empirical data. The research results significantly contribute to understanding the topic and enable the researcher to derive meaningful conclusions. Furthermore, an analysis of the implications of the findings is conducted, emphasising their importance within the overall framework of this research study. Additionally, recommendations for future research, suggesting avenues for further exploration and investigation, are provided.

In order to present a thorough viewpoint, constraints that were encountered throughout the course of this investigation are deliberately recognised. Furthermore, possible avenues for future research are contemplated, thereby ensuring that the pursuit of knowledge persists.

## 6.2 Discussion and implications of the findings

To stay ahead in the ongoing battle against cyber dangers, individuals and businesses can gain a competitive edge by thoroughly exploring the implications of the cybersecurity findings highlighted in this study. Consequently, addressing these findings will lead to systems that are more resistant to disruptions, policies that are enhanced, and a digital environment that is more secure.

Based on the analysis conducted in this study, it appears that employees within the organisation do not seem to have access to IT security policies. Employees may be uncertain about how to find these policies for reference. The literature review conducted for this study found that access control systems that are not configured properly can create loopholes that malicious actors can use to gain access to sensitive data and systems. This can lead to data theft, system compromise, and other malicious activities.

The finding that certain employees lack the necessary expertise to identify and differentiate cyberattacks highlights an essential cybersecurity concern. Based on the survey results, certain individuals are unsure if they have encountered any attempted attacks. This uncertainty can be attributed to inadequate training, expertise, and

resources related to recognising potential exploits. In the absence of adequate training, these individuals may lack the ability to identify or address potential vulnerabilities promptly. The literature review conducted for this study revealed that training and education programs develop a security culture and alert employees of potential hazards. They also teach employees how to spot and respond to suspicious behaviour to safeguard themselves and their companies.

The findings presented that employees are able to access work data from personal computers or devices, which poses a cybersecurity risk in the sense that personal devices generally lack the equivalent levels of security measures, policies, and configurations as devices managed by the organisation. Consequently, the personal device may become infected with harmful software, thereby compromising the security of the company's data.

The findings indicating extensive utilisation of social media platforms for sharing corporate data indeed raise significant security concerns. Examining and ensuring that this practice aligns with security policies and standards is crucial. Social media platforms are easily accessible, allowing employees to share confidential information with just about anyone. According to the literature, the global problem of corporate data being shared on social media presents substantial hazards to corporations. It is possible for information that is vital to a business to be compromised as a result of employee activities on social media networks. Without proper security measures in place, this can lead to data breaches and leaks that can have serious consequences for the business. It is, therefore, essential that companies review their security policies and ensure that they are in line with current best practices.

## 6.3 An Awareness Model for the use of IT Security Policies

As shown in *Figure 6.1* below, an awareness model for the use of Information Technology Security Policies in the Petroleum Retail Sector in South Africa has been developed. This model was derived using findings from the literature, a TOE framework and insights from data collected.

The model in *Figure 6.1* provides a five-step structured approach to developing, implementing and usage of IT Security Policies in the petroleum retail sector. It highlights the importance of understanding the governance requirements associated with IT

security policies. It also highlights the need to create a culture of safety and security. The model also emphasizes the importance of controls in place to protect the organisation and regularly monitoring and reviewing policies and the threat landscape. This is to ensure the organisation remains relevant and effective when it comes to IT Security.

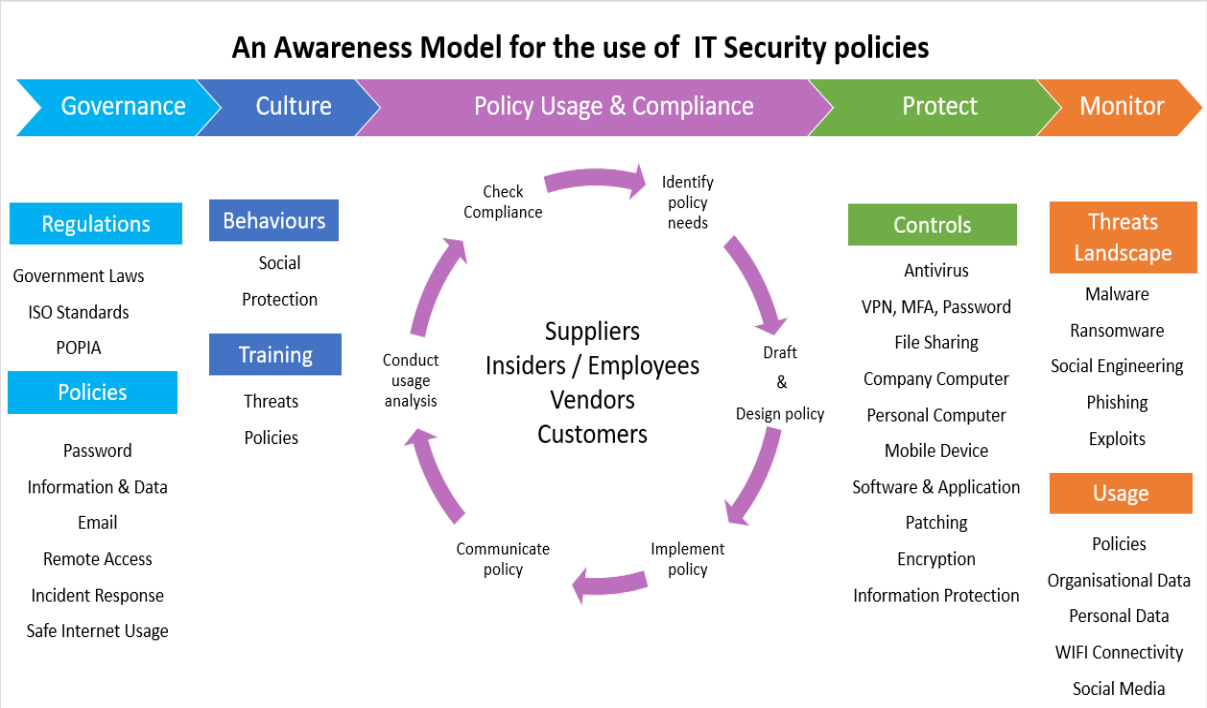



*Figure 6.1 An Awareness Model for the use of IT Security Policies*

## 6.4 Importance of further exploration

- Future research should prioritize the investigation of the influence of access management on the security of digital assets, the examination of how access management can be utilized to counteract cyber threats, and the formulation of strategies to reduce risks connected with access management. Furthermore, it is important to do research that specifically examines the economic impact of access management and provide insights into how organisations should strategically make investments in resources that minimize such risks. Access management is crucial in safeguarding digital assets against cyber threats, and companies must understand how to deploy resources to effectively manage the related risks. Moreover, comprehending the economic ramifications of access

management can assist firms in making well-informed decisions regarding risk management.

- Future research should focus on investigating insider risks in access management and developing strategies that utilise behavioral analytics to effectively detect and prevent suspicious acts by insiders, while allowing legitimate users to access data.
- The finding around lack of employee expertise in detecting and distinguishing cyberattacks is a significant issue in today's digital environment. Further research in this field could explore different aspects, including assessing the efficacy of current cybersecurity training programs for employees, creating role-specific cybersecurity training programs, and developing metrics to gauge employees' awareness and readiness in cybersecurity.
- The practice of employees accessing work data from personal devices poses notable challenges and opportunities for further investigation in research regarding the effectiveness of current policies in reducing security risks, evaluating the efficacy of Bring Your Own Device (BYOD) in safeguarding work data on personal devices, and examining the impact of remote work culture and flexibility on employee behavior and security protocols.
- The extensive utilisation of social media platforms to share corporate data raises significant security concerns and necessitates additional research to evaluate the efficacy of current security policies and governance frameworks in mitigating the risks associated with sharing corporate data on social media.

## 6.5 Significance of the findings

Access management is essential in cybersecurity as it governs and oversees the authorization of individuals to specific information within a system or organization. The significance of it lies in several critical categories.

- **Data Protection:** Access management guarantees that confidential data can only be accessed by authorized personnel. This mitigates the likelihood of data breaches and unauthorized access or alteration of crucial information (Devlekar & Ramteke, 2021).

- **Risk Mitigation:** Organisations can reduce the likelihood of insider threats or unauthorized external access by implementing access rights management. By restricting access, the likelihood of malicious activities or unintended harm is reduced. (Afshar et al., 2021).
- **Compliance and regulations:** Numerous industries enforce strong compliance obligations, such as GDPR and HIPAA. Access management facilitates organizational compliance with these requirements by ensuring that data is accessed and managed in accordance with specified guidelines (Thapa & Camtepe, 2021).
- **Enhanced Security:** Proper access management strengthens overall security posture by implementing measures such as multi-factor authentication, least privilege principles, and regular access reviews. This makes it harder for attackers to gain unauthorized access (Vidyasagar & Murugan, 2021).

The ability to detect and differentiate cyberattacks is of the utmost importance in maintaining a strong cybersecurity defense. Their contributions to different elements of cyber defense are as follows:

- **Rapid detection**: Enables prompt reaction and confinement, so minimizing the possible harm resulting from an attack. The ability to differentiate between various forms of attacks facilitates the implementation of targeted mitigation strategies, thereby minimizing their adverse effects on systems, data, and operations (Aktukmak et al., 2021).
- **Preserving data integrity:** It is essential to distinguish between attacks that seek to corrupt or manipulate data and those that concentrate on disrupting the system. Ensuring the accuracy and reliability of data is of utmost importance, and understanding the type of attack helps in establishing measures to safeguard against unauthorized tampering of data (Tian & Nogales, 2023).
- **Adapting to Evolving Threats:** Since cyber threats evolve continuously. Detection and differentiation facilitate maintaining a competitive edge through the comprehension of innovative attack vectors, techniques, and patterns. Acquiring this knowledge is of the utmost importance when it comes to updating security protocols and tools in order to effectively defend against emerging threats (Jawad & Hlayel, 2022).

## 6.6 Contributions

The research study is expected to potentially produce the following outcomes:

- The proposed recommendations that could lead to an improvement in compliance and the adoption of IT security policies in the petroleum retail sector.
- Besides the petroleum retail sector, there are other sectors of the economy that can benefit from this study as well
- The results of this study have been submitted as an article for publication in a peer-reviewed journal. The manuscript is currently undergoing review, and the authors expect to receive a response soon. If accepted, the article will be published and made available to the general public.

### 6.6.1 Practical contributions

The following practical contributions are vital for addressing the challenges that are presented by non-compliance behaviours:

- **Data Encryption and Access Management Best Practices:** Encouraging the use of data encryption best practices while sharing private information on social media. This involves teaching staff members the proper encryption techniques to safeguard data from unauthorised access.
- **Ongoing Training and Awareness Programs:** Information professionals and employees alike should recognise the importance of ongoing security training and awareness programs. Practical contributions in this regard involve developing and implementing effective training modules that educate employees about the risks associated with social media usage and best practices for data protection.
- Assisting IT security managers and specialists to drive IT security compliance and encourage the use of IT Security policies
- Assisting the petroleum retail organisation to protect its information and information systems against insider threats
- Assisting the petroleum retail organisation to avoid disruption, reputational damage, penalties, and loss of business
- An awareness model that assists with security policy compliance and adoption

## 6.7 Authentication

**Utilizing strong and not easy to guess passwords is essential to protect me from cyber-attacks.**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Agree | 8 | 11.9 | 11.9 | 11.9 |
| | Strongly agree | 59 | 88.1 | 88.1 | 100.0 |
| | Total | 67 | 100.0 | 100.0 | |

*Figure 6.2 Utilising strong password*

**Which MFA or two-factor authentication method do you find best to use usage?**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | I don't know | 1 | 1.5 | 1.5 | 1.5 |
| | Phone call | 2 | 3.0 | 3.1 | 4.6 |
| | SMS Code | 19 | 28.4 | 29.2 | 33.8 |
| | Authentication App | 43 | 64.2 | 66.2 | 100.0 |
| | Total | 65 | 97.0 | 100.0 | |
| Total | | 67 | 100.0 | | |

*Figure 6.3 MFA methods*

### *1. Utilising strong password*

**Error! Reference source not found.** and **Error! Reference source not found.** present the use of authentication methods, especially the use of passwords—the MFA methods. **Error! Reference source not found.** indicates significant agreement among employees regarding the importance of utilising strong passwords for authentication. This consensus indicates that the implementation of robust passwords may not be a major area of concern when it comes to compliance with cybersecurity policies. The strong

agreement among employees, as shown in **Error! Reference source not found.** on the importance of robust passwords suggests that employees are well-prepared to protect organisational data through the use of strong passwords.

The high level of awareness and understanding among employees about the critical role strong passwords play in enhancing cybersecurity is a positive sign. It suggests that the organisation has successfully instilled a cybersecurity-conscious culture among its workforce around strong passwords. Employees appear to be well-informed about the potential risks associated with weak passwords and the importance of adhering to best practices in password security. While the findings indicate positive compliance with using strong passwords, it is important for the organisation to continue promoting and reinforcing good password practices. Periodic training and awareness programs can serve as effective reminders to ensure that employees consistently employ strong passwords and remain vigilant against potential threats.

***2. Two-Factor Authentication Methods***

**Prominence of Modern Methods**: The prominence of modern authentication methods, particularly the preference for authentication apps and SMS codes over other options, indicates that employees are embracing and finding comfort in the use of these contemporary two-factor authentication methods.

The positive response towards authentication apps and SMS codes suggests that employees are receptive to new technological advancements in the realm of cybersecurity. They appear to value the convenience and ease of use offered by these modern methods.

The preference for these modern methods may also be indicative of employees' awareness of the potential security benefits they offer. Authentication apps and SMS codes are generally considered more secure than traditional email-based or phone-based authentication methods. They provide an additional layer of protection against unauthorised access and mitigate the risks associated with password-only authentication.

**Education Opportunity**: The small percentage of employees who do not know their preferred authentication method represents a valuable education opportunity for the

organisation. This group of individuals may be unfamiliar with the available options or uncertain about which method would best suit their needs.

The group of employees, which constitutes 1.5% as shown in **Error! Reference source not found.** who do not know their preferred authentication method represents a valuable target on cybersecurity threats, implications, and consequences of cybersecurity threats. The lack of knowledge or awareness among these employees could be due to the job description or lack of familiarity with technological devices. It is, therefore, imperative for the organisation to provide a medium of education and guidance through periodical training on cybersecurity vulnerability. The organisation can empower employees to make informed choices and strengthen their commitment to cybersecurity best practices by offering targeted guidance, training resources, and user-friendly interfaces. Through ongoing communication and incentives, the organisation can create a security-aware culture where all employees actively participate in selecting and using their preferred authentication method to safeguard sensitive data and protect against potential security threats.

### 6.7.1 Theoretical contributions

The following theoretical contributions are crucial to the advancement of cybersecurity as they offer the foundation for future investigations, the creation of new methods and technologies, and the improvement of cybersecurity knowledge and capacities as a whole:

- **Cybersecurity Culture:** A theoretical framework that explores the influence of company culture on shaping employees' cybersecurity practices and behaviours.
- **Risk Assessment:** An innovative theoretical framework that incorporates a risk assessment that considers not just technical vulnerabilities but also human aspects, behaviours, psychology, and the wider organisational context, thereby offering a more comprehensive perspective on cybersecurity risk.
- **Security Information Sharing:** An integrated framework that facilitates efficient sharing of security information and threat intelligence among organisations, including social media platforms, thereby enhancing collaborative defence against cyber threat

## 6.8 Limitations

This study possesses certain limitations that need acknowledgement:

- **Sample Size:** Interviewing all sectors and employees in the petroleum retail industry presented challenges due to constraints such as limited time and budget. Therefore, a sampling technique was applied to collect data and obtain representative insights.
- **Inadequate Real-World Testing:** To obtain a comprehensive understanding of cybersecurity research associated with compliance and adoption, it may be necessary to conduct simulations that test various situations. Subsequently, it is important to note that this study does not completely match real-world conditions and behaviours, which can impact the generalizability of its conclusions.

## 6.9 Recommendations

Based on the finding that employees within the organisation do not seem to have access to IT security policies and that certain employees lack the necessary expertise to identify and differentiate cyberattacks, it is critical to ensure that all staff members have access to the latest security policies and that regular training is being conducted to ensure that employees understand the importance of using IT security policies and where to access them.

Based on the finding that employees access work data from personal computers, organisations can strengthen their access management practices and overall cybersecurity posture by utilising the TOE framework to address and assess policies, patching, authentication, firewall measures and manage company data accessed via personal computers, which is essential in safeguarding sensitive data and information.

Based on the finding that there is extensive utilisation of social media platforms for sharing corporate data by employees, the establishment of explicit standards to ensure compliance behaviours are performed is critical. Organisations should develop and

implement a comprehensive data-sharing policy that outlines the types of data to be shared, how it should be shared, and who is authorised to access it. Additionally, organisations should educate their employees on the importance of secure data-sharing and the potential risks associated with it.

Fostering collaboration between IT and non-IT departments is essential to establish collective accountability for cybersecurity. This may be achieved by encouraging close collaboration between IT and non-IT teams to address cybersecurity concerns and provide guidance. This will help to ensure that everyone in the organisation is on the same page when it comes to understanding the importance of cybersecurity and that they are taking the necessary steps to protect their data and systems. It will also create an environment of trust and collaboration, which is essential for any successful security program.

It is critical to provide thorough cybersecurity training to all employees through their onboarding process, as well as periodic refresher training, irrespective of their job responsibilities. This training should cover the basics of identifying common cyber threats, phishing emails, social engineering tactics, and best practices for online security. Regular awareness programs and updates can reinforce this knowledge. As cyber threats continue to evolve, it is essential that employees across all units remain informed about the latest methods and comprehensive vulnerabilities that are being employed.

Investments in cybersecurity tools, software and upgrades of cybersecurity infrastructures that can detect and prevent cyber threats are essential, such as email filtering solutions, anti-malware software, intrusion detection systems, backup systems and endpoint security software. These solutions can help detect malicious emails, protect networks from malware, and prevent unauthorised access to systems, respectively.

Implementing a compliance and adoption framework allows the oil and gas industry to effectively manage cybersecurity risks, comply with regulations, preserve sensitive data, improve operational safety, protect critical infrastructure, and uphold a robust cybersecurity stance. Moreover, implementing a compliance and adoption framework can assist firms in reducing financial and legal liabilities and mitigating harm to their brand. Additionally, it can aid firms in establishing trust with stakeholders, customers, and shareholders

## 6.10 Conclusion

The conclusions are based on the research questions in section 1.6 and the corresponding research objectives in section 1.7.

***MRQ: How can an awareness model be developed to improve the use of IT security policies in the petroleum retail sector?***

***MRO: To develop an awareness model for the use of Information Technology security (IT security) policies in the petroleum retail sector.***

Chapter 5 of this study provides an awareness model for the use of IT security policies. The model is based on a questionnaire provided to petroleum retail employees, both technical and non-technical. The model provides a framework that assists organisations with compliance to IT security policies.

**SQ1: What IT security controls or policies are in place to protect organisational information?**

***SO1: To determine IT security policies and controls that are in place to protect organisational information.***

The findings in this study, which have been presented in Chapter 5, highlight the following: Access management, authentication protocols, cybersecurity knowledge, cybersecurity capacity development, and adopting synergy in data sharing and compliance. In relation to access management, the use of personal devices does not enjoy a general consensus. It is noteworthy to indicate that the use of personal devices relates to accessing organisational information, which could make sensitive IT infrastructure vulnerable to cybersecurity. The coordination of access management in the context of the use of personal devices (accessing sensitive information on personal devices) use of publicly available internet facilities, which in most cases do not enjoy stringent cybersecurity protocols, therefore implies that several protocols such as raising awareness, develop, and implement mobile device policies, monitor, and enforce policy compliance as well as periodic security audits in the form of risk assessment have been identified in this study.

**SQ2: What organisational factors are used to promote IT security policy compliance and adoption?**

***SO2: To explore organisational factors used to promote IT security policy compliance***

**Authentication and knowledge**

The importance of a robust authentication procedure as an organisational factor was revealed by participants, such that using two-factor authentication as well as strong passwords and SMS codes were some of the most preferred methods of authentication. In essence, participants demonstrated adequate interest in protecting and safeguarding vulnerable IT infrastructure from cybersecurity threats, with their preference for using these methods to promote the use of IT policies. It is important that sustaining this culture is important for the organisation to continue promoting and reinforcing good password practices. Periodic training and awareness programs can serve as effective reminders to ensure that employees consistently employ strong passwords and remain vigilant against potential threats.

**SQ3: What challenges are experienced with IT security compliance in the organisation?**

***SO3: To discover challenges experienced with IT security policies in the organisation***

**Security, training, data sharing and compliance**

The severity of cybersecurity is one of the challenges identified in this study. Also, the lack of comprehensive training, coordinated data-sharing protocols and the importance of compliance are some of the additional challenges. This study shows that participants demonstrate a lack of adequate cybersecurity threats and, by extension, the willingness to attend training on the industry cybersecurity threats. In addition, compliance, especially in using industry-designated security protocols, was observed to be another organisational factor because, in some cases, employees are unaware of the hacking attempts on their devices, hence inadequate data sharing information. It implies that organisations must develop reporting protocols for employees on suspicious cybersecurity threat activity.

## 6.11 Summary

This paper delves into the literature, findings and recommendations of the study. It highlights the critical issues in the petroleum retail sector, such as employees lacking access to IT security policies, risking data theft and system compromise. Moreover, employees accessing work data from personal devices and the extensive use of social media for corporate data sharing pose significant security concerns. The lack of training and expertise in identifying cyberattacks and risks is a substantial concern.

This research paper also highlights the implications arising from the findings of this study. and suggests several possibilities for further investigation.

The importance of establishing IT security policies and providing comprehensive training to safeguard organisational information is stressed. Access management practices should be strengthened, and data-sharing policies should be implemented. Collaboration between IT and non-IT departments is essential for collective accountability.

## REFERENCES


Aktukmak, M., Yilmaz, Y. and Uysal, I., 2021. Sequential attack detection in recommender systems. *IEEE Transactions on Information Forensics and Security*, *16*, pp.3285-3298.

Arfeen, A., Ahmed, S., Khan, M.A. and Jafri, S.F.A. (2021). Endpoint Detection & Response: A Malware Identification Solution. *2021 International Conference on Cyber Warfare and Security (ICCWS)*. doi:https://doi.org/10.1109/iccws53234.2021.9703010.

Al-Ababneh, M.M. (2020). Linking Ontology, Epistemology and Research Methodology. *Science & Philosophy*, 8(1), pp.75–91. doi:https://doi.org/10.23756/sp.v8i1.500.

Aldawood, H. and Skinner, G., 2019. Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet*, *11*(3), p.73.

Al-Sarawi, S., Anbar, M., Abdullah, R. and Al Hawari, A.B. (2020). *Internet of Things Market Analysis Forecasts, 2020–2030*. [online] IEEE Xplore. doi:https://doi.org/10.1109/WorldS450073.2020.9210375.

Alsulami, M.H., Alharbi, F.D., Almutairi, H.M., Almutairi, B.S., Alotaibi, M.M., Alanzi, M.E., Alotaibi, K.G. and Alharthi, S.S. (2021). Measuring Awareness of Social Engineering in the Educational Sector in the Kingdom of Saudi Arabia. *Information*, 12(5), p.208. doi:https://doi.org/10.3390/info12050208.

Alghamdi, A. A., 2021. *Overview of Cybersecurity Challenges in Fourth Industrial Revolution.*

Alturki, R. (2021). Research Onion for Smart IoT-Enabled Mobile Applications. *Scientific Programming*, [online] 2021(1), pp.1–9. doi:https://doi.org/10.1155/2021/4270998.

Alsowail, R.A. and Al-Shehari, T., 2020. Empirical detection techniques of insider threat incidents. *IEEE Access*, *8*, pp.78385-78402.

Afshar, M., Samet, S. and Usefi, H., 2021, April. Incorporating behavior in attribute based access control model using machine learning. In *2021 IEEE International Systems Conference (SysCon)* (pp. 1-8). IEEE.

AKKAYA, B. (2023). Grounded Theory: A Comprehensive Examination of Data Coding. *International Journal of Contemporary Educational Research*. doi:https://doi.org/10.33200/ijcer.1188910.

Amini, M., 2023. *A Multi-Perspective Framework Established on Diffusion of Innovation (DOI) Theory and Technology, Organization and Environment (TOE) Framework Toward Supply Chain Management System.*

Armstrong Lee Agbaji (2021). An Empirical Analysis of Artificial Intelligence, Big Data and Analytics Applications in Exploration and Production Operations. doi:https://doi.org/10.2523/iptc-21312-ms.

Aslan, Ö., Aktuğ, S.S., Ozkan-Okay, M., Yilmaz, A.A. and Akin, E., 2023. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), p.1333.

Atkins, S. (2023). The ethics of engagement. *Journal of Applied Linguistics and Professional Practice*. doi:https://doi.org/10.1558/jalpp.20074.

Basare, A., Bhojak, D. and Solanki, Dr.R. (2023). Biometric Authentication System. *International Journal for Research in Applied Science and Engineering Technology*, [online] 11(6), pp.3232–3238. doi:https://doi.org/10.22214/ijraset.2023.54246.

Bazarkina, D. and Pashentsev, E., 2020. Malicious use of artificial intelligence. *Russia in Global Affairs*, *18*(4), pp.154-177.

Bianchi, L.M., 2022. Obtaining Informed Consent for Research Studies. In *Research During Medical Residency* (pp. 139-156). CRC Press.

Bote, D., 2019. *The South African National Cyber Security Policy Framework: A critical analysis.*

Branaghan, R.J., O'Brian, J.S., Hildebrand, E.A. and L. Bryant Foster (2021). *Humanizing Healthcare – Human Factors for Medical Device Design*. *Springer eBooks*. Springer Nature. doi:https://doi.org/10.1007/978-3-030-64433-8.

Bukowska, M. (2021). Critical realism: one of the main theoretical orientations of the social sciences in the twentieth and twenty-first centuries. *Journal of Critical Realism*, 20(4), pp.441–447. doi:https://doi.org/10.1080/14767430.2021.1975212.

Campos Pinto, P. and Hickey, H., 2023. Qualitative Research: Introduction. In *Handbook of Disability: Critical Thought and Social Change in a Globalizing World* (pp. 1-5). Singapore: Springer Nature Singapore.

Chandra P Jain, S. S. & Nanda Kumar P Jain, K. S., 2018. *Exploring Factors Influencing Organisational Adoption Of Augmented Reality In E-Commerce: Empirical Analysis Using Technology-Organization-Environment Model.*

Connor Desai, S. and Reimers, S. (2018). Comparing the use of open and closed questions for Web-based measures of the continued-influence effect. *Behavior Research Methods*, [online] 51(1). doi:https://doi.org/10.3758/s13428-018-1066-z.

Danet, D., 2020. *Punish and Perish: The Human Factor in Cybersecurity.*

Dash & Ansari, 2022. *An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy.*

Depietro, R., Wiarda, E. and Fleischer, M., 1990. The context for change: Organisation, technology and environment. *The processes of technological innovation*, *199*(0), pp.151-175.

Devlekar, S. and Ramteke, V., 2021. Identity and Access Management: High-level Conceptual Framework. *REVISTA GEINTEC-GESTAO INOVACAO E TECNOLOGIAS*, *11*(4), pp.4885-4897.

Dissanayake, N., Jayatilaka, A., Zahedi, M. and Ali Babar, M. (2020). *Software Security Patch Management -A Systematic Literature Review of Challenges, Approaches, Tools and Practices*. [online] Available at: https://arxiv.org/pdf/2012.00544.pdf.

Dudovskiy, J. (2019). *Deductive Approach (Deductive Reasoning) - Research-Methodology*. [online] Research-Methodology. Available at: https://research-methodology.net/research-methodology/research-approach/deductive-approach-2/.

Eriksson, D. and Engström, A. (2021). Using critical realism and abduction to navigate theory and data in operations and supply chain management research. *Supply Chain Management: An International Journal*, 26(2), pp.224–239. doi:https://doi.org/10.1108/scm-03-2020-0091.

Etim, E. (2021). *Information Technology/Information Systems Adoption in Developing and Transitioning Economies*. [online] www.igi-global.com. Available at: https://www.igi-global.com/chapter/information-technologyinformation-systems-adoption-in-developing-and-transitioning-economies/264984.

Festinger, D.S., Dugosh, K.L., Callahan, H.R. and Hough, R.A. (2023). *Informed Consent to Research*. [online] Cambridge University Press. Available at: https://www.cambridge.org/core/books/abs/cambridge-handbook-of-research-methods-and-statistics-for-the-social-and-behavioral-sciences/informed-consent-to-research/649DDE8015EE1ADBC3247C5EC1332A04.

Galliers, Robert. (1991). Choosing Appropriate Information Systems Research Approaches: A Revised Taxonomy. *The Information Research Arena of the 90s,* pp.155–173.

Gandeva Bayu Satrya, Niken Dwi Wahyu Cahyani and Andreta, R.F. (2015). The Detection of 8 Type Malware botnet using Hybrid Malware Analysis in Executable File Windows Operating Systems. doi:https://doi.org/10.1145/2781562.2781567.

Gautam, D. and Tokekar, V. (2020). A novel Approach for Detecting DDoS Attack in MANET. *Materials Today: Proceedings*, 29, pp.674–677. doi:https://doi.org/10.1016/j.matpr.2020.07.332.

Genfer, P., Zdun, U. (2022). Avoiding Excessive Data Exposure Through Microservice APIs. In: Gerostathopoulos, I., Lewis, G., Batista, T., Bureš, T. (eds) *Software Architecture*. ECSA 2022. Lecture Notes in Computer Science, vol 13444. Springer, Cham. https://doi.org/10.1007/978-3-031-16697-6_1.

Georgi Tsochev, et al., 2020. *Cyber security: Threats and Challenges.*

Gross, H. et al., 2020. *Information Security Policy Compliant and Noncompliant Behaviors of Non-It Organizational Personnel.*

Gundu, S.R., Panem, C.A. and Thimmapuram, A., 2020. Hybrid IT and multi cloud an emerging trend and improved performance in cloud computing. *SN Computer Science*, *1*(5), p.256.

Hale, M.L. and Gamble, R.F., 2019. Semantic hierarchies for extracting, modeling, and connecting compliance requirements in information security control standards. *Requirements Engineering*, *24*, pp.365-402.

Hamilton, L. and Rauch, M. (2022). The oil and gas cybersecurity enigma. *The Leading Edge*, 41(9), pp.641–646. doi:https://doi.org/10.1190/tle41090641.1.

Hamdani, S.W.A., Abbas, H., Janjua, A.R., Shahid, W.B., Amjad, M.F., Malik, J., Murtaza, M.H., Atiquzzaman, M. and Khan, A.W. (2021). *Cybersecurity Standards in the Context of Operating System. ACM Computing Surveys, 54(3), pp.1–36. doi:https://doi.org/10.1145/3442480.*

Haro, J.E., Elisabete Ramalho, and Guillermo de (2017). *To Improve Cybersecurity, Think Like a Hacker*. [online] MIT Sloan Management Review. Available at: https://sloanreview.mit.edu/article/to-improve-cybersecurity-think-like-a-hacker/.

Hasan, S., Ali, M., Kurnia, S. and Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, [online] 58, p.102726. doi:https://doi.org/10.1016/j.jisa.2020.102726.

Hassan, M., Jincai, C., Iftekhar, A., Shehzad, A. and Cui, X., 2020. Implementation of security systems for detection and prevention of data loss/leakage at organization via traffic inspection. *arXiv preprint arXiv:2012.14111*.

Hewlett, L. and Werbeloff, M. (2022). Preparing public management students for mixed methods research. *Teaching Public Administration*, p.014473942211103. doi:https://doi.org/10.1177/01447394221110339.

T. Honeycutt, W., Kim, T., Tyler Ley, M. and F. Materer, N. (2021). Sensor array for wireless remote monitoring of carbon dioxide and methane near carbon sequestration and oil recovery sites. *RSC Advances*, [online] 11(12), pp.6972–6984. doi:https://doi.org/10.1039/D0RA08593F.

Hoofnagle, C.J., Sloot, B.V.D. and Borgesius, F.Z. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, [online] 28(1), pp.65–98. doi:https://doi.org/10.1080/13600834.2019.1573501.

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y. and Ochoa, M. (2019). Insight Into Insiders and IT. *ACM Computing Surveys*, 52(2), pp.1–40. doi:https://doi.org/10.1145/3303771.

Hussain, R.F., Mokhtari, A., Ghalambor, A. and Salehi, M.A. (2022). *IoT for Smart Operations in the Oil and Gas Industry: From Upstream to Downstream*. [online] *Google Books*. Gulf Professional Publishing. Available at: https://books.google.co.za/books?hl=en&lr=&id=9n9dEAAAQBAJ&oi=fnd&pg=PP1&dq.

Jalali, A., Assadi, L. and Osman, A. (2023). *Password Management A Study about Current Challenges with Password Management*. [online] Available at: https://www.divaportal.org/smash/get/diva2:1765652/FULLTEXT01.pdf

Jawad, M.S. and Hlayel, M., 2022. Intelligent Cybersecurity Threat Management in Modern Information Technologies Systems. In *Lightweight Cryptographic Techniques and Cybersecurity Approaches*. IntechOpen.

Joshi, S., Munjal, S. and Karanje, U.B., 2019. Gas Leakage Detection and Alert System using IoT. *Article in International Journal of Scientific Research in Science and Technology*.

Karupiah, P. (2022). Positivism. *Principles of Social Research Methodology*, pp.73–82. doi:https://doi.org/10.1007/978-981-19-5441-2_6.

Kävrestad, J., Eriksson, F. and Nohlberg, M. (2019), "Understanding passwords – a taxonomy of password creation strategies", *Information and Computer Security*, Vol. 27 No. 3, pp. 453-467. https://doi.org/10.1108/ICS-06-2018-0077

Kennedy, E.B., Jensen, E.A. and Jensen, A.M., 2022. Methodological Considerations for Survey-Based Research During Emergencies and Public Health Crises: Improving the Quality of Evidence and Communication. *Frontiers in Communication*, *6*, p.736195.

Khan, N., J. Houghton, R. and Sharples, S. (2021). Understanding factors that influence unintentional insider threat: a framework to counteract unintentional risks. *Cognition, Technology & Work*. doi:https://doi.org/10.1007/s10111-021-00690-z.

Klein, G. and Zwilling, M. (2023). The Weakest Link: Employee Cyber-Defense Behaviors While Working from Home. pp.1–15. doi:https://doi.org/10.1080/08874417.2023.2221200.

Komal, U. (2023). Data Leakage Detection using Cloud Computing. *International Journal for Research in Applied Science and Engineering Technology*, [online] 11(5), pp.3129–3132. doi:https://doi.org/10.22214/ijraset.2023.52273.

Kraft, A.K., Maag, C. and Baumann, M., 2020. Comparing dynamic and static illustration of an HMI for cooperative driving. *Accident Analysis & Prevention*, *144*, p.105682.

Kshetri, N. (2013). *Global Cybersecurity: Issues and Concern*. [online] papers.ssrn.com. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2350422.

Liamputtong, P. (2023). *Qualitative research in the social sciences: setting the scene*. [online] www.elgaronline.com. Available at: https://www.elgaronline.com/edcollchap/book/9781800376199/book-part-9781800376199-7.xml.

Liu, K., Xie, Y., Xie, S. and Sun, L. (2023). SEAG: A novel dynamic security risk assessment method for industrial control systems with consideration of social engineering. *Journal of Process Control*, [online] 132, p.103131. doi:https://doi.org/10.1016/j.jprocont.2023.103131.

M Van Lange Arie W Kruglanski, P. A., Tory Higgins Volume, E. & Lange, V., 2012. *Handbook of Theories of Social Psychology.*

*Magalhães, M., Pereira, T.C., Costa, E., Agostinho Sousa Pinto, José Luís Braga and Borges, I. (2023). DPO Framework for Canvas GDPR Model. Smart innovation, systems and technologies, pp.93–109. doi:https://doi.org/10.1007/978-981-19-9960-4_10.*

Mahlobo, D. & David, M., 2015. *The National Cybersecurity Policy Framework (NCPF)*.

Masrek, M. N., Soesantari, T., Khan, A. & Dermawan, A. K., 2020. *Examining The Relationship Between Information Security Effectiveness And Information Security Threats.*

Masuduzzaman, M., Mahmud, A., Islam, A. and Islam, M.M., 2020. Two Phase Authentication and VPN Based Secured Communication for IoT Home Networks. *Safety, Security, and Reliability of Robotic Systems*, pp.131-140.

Mehra, A. and Badotra, S. (2021). *Artificial Intelligence Enabled Cyber Security*. [online] IEEE Xplore. doi:https://doi.org/10.1109/ISPCC53510.2021.9609376.

Meier, S., Fuchs, L. and Pernul, G. (2013). Managing the Access Grid - A Process View to Minimize Insider Misuse Risks. *Wirtschaftsinformatik Proceedings 2013*. [online] Available at: https://aisel.aisnet.org/wi2013/66/

Meyer, L., Romero, S., Bertoli, G., Burt, T., Weinert, A. and Ferres, J. (n.d.). *HOW EFFECTIVE IS MULTIFACTOR AUTHENTICATION AT DETERRING CYBERATTACKS?* [online] Available at: https://arxiv.org/pdf/2305.00945.pdf.

Mittal, A. and Garg, U. (2022). A review for insider threats detection using machine learning. *AIP Conference Proceedings*. [online] doi:https://doi.org/10.1063/5.0108887.

Mohajan, H., 2020. *Munich Personal RePEc Archive Quantitative Research: A Successful Investigation in Natural and Social Sciences.*

Mahomed, S., Loots, G. and Staunton, C. (2022). *The role of Data Transfer Agreements in ethically managing data sharing for research in South Africa. South African Journal of Bioethics and Law, pp.26–30. doi:https://doi.org/10.7196/sajbl.2022.v15i1.807.*

Moradbeikie, A., Jamshidi, K., Bohlooli, A., Garcia, J. and Masip-Bruin, X., 2020. An IIoT based ICS to improve safety through fast and accurate hazard detection and differentiation. *IEEE access*, *8*, pp.206942-206957.

Nassaji, H., 2020. Good qualitative research. *Language Teaching Research*, *24*(4), pp.427-431.

Ndame, T. (2023). Case Study. *Springer texts in education*, pp.67–72. doi:https://doi.org/10.1007/978-3-031-04394-9_11.

Olvera-Arellano, A.G. (2022). Strengthen the autonomy of the research subject by protecting their personal data. *Mexican Bioethics Review ICSA*, 4(7), pp.21–26. doi:https://doi.org/10.29057/mbr.v4i7.8525.

Onu, E., Kwakye, M.M. and Barker, K., 2020, August. *Contextual privacy policy modeling in IoT. In 2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech) (pp. 94-102).*

Patel, M. and Patel, N., 2019. Exploring research methodology. *International Journal of Research and Review*, *6*(3), pp.48-55.

Pandey, P. & Pandey, M. M., 2015. *Research methodology: Tools & techniques.*

Park, Y.S., Konge, L. and Artino, A.R. (2020). The Positivism Paradigm of Research. *Academic Medicine*, [online] 95(5), pp.690–694. doi:https://doi.org/10.1097/ACM.0000000000003093.

Parsoya, S. & Perwej, A., 2021. *Significance of Technology and Digital Transformation in Shaping the Future of Oil and Gas Industry.*

Pietilä, A.-M., Nurmi, S.-M., Halkoaho, A. and Kyngäs, H. (2020). Qualitative Research: Ethical Considerations. *The Application of Content Analysis in*

*Nursing Science Research*, [online] 1(1), pp.49–69. Available at: https://link.springer.com/chapter/10.1007/978-3-030-30199-6_6.

Ponce, O.A., Gómez-Galán, J. and Pagán-Maldonado, N., 2022. Qualitative research in education: revisiting its theories, practices and developments in a scientific-political era.

Prostean, G. et al., 2020. *Security and Privacy Implementation Framework as a Result of the Digitalization Process for Organizations in Different Industries. Springer proceedings in business and economics.*

Radhika Mohan Gupta, Mathur, P. and Nanda, R. (2022). Cyber Security Threat, it's Risks and Susceptibilities, in the Global Perspective. *Lecture notes in networks and systems*, pp.607–613. doi:https://doi.org/10.1007/978-981-19-1122-4_63.

Ragab, M. and Altalbe, A. (2022). A Blockchain-Based Architecture for Enabling Cybersecurity in the Internet-of-Critical Infrastructures. *Computers, Materials & Continua*, 72(1), pp.1579–1592. doi:https://doi.org/10.32604/cmc.2022.025828.

Raghavendra, M., Omprakash, P. and B R, M. (2021). AuthNet: A Deep Learning Based Authentication Mechanism Using Temporal Facial Feature Movements (Student Abstract). *Proceedings of the AAAI Conference on Artificial Intelligence*, 35(18), pp.15873–15874. doi:https://doi.org/10.1609/aaai.v35i18.17933.

Rashid, A. et al., 2018. *Scoping the Cyber Security Body of Knowledge.*

Raul, A.C. ed., 2021. *The privacy, data protection and cybersecurity law review*. Law Business Research Limited.

Rawal, B.S., Gunasekaran Manogaran and Peter, A. (2023). *Cybersecurity and Identity Access Management*. doi:https://doi.org/10.1007/978-981-19-2658-7.

Reid, P.E. (2020). *Facility Manager's Guide to Security: Protecting Your Assets*. [online] *Google Books*. Available at: https://books.google.co.za/books?hl=en&lr=&id=4xkOEAAAQBAJ&oi=fnd&pg=PP1&dq.

Ren, Y., Cedeno-Mieles, V., Hu, Z., Deng, X., Adiga, A., Barrett, C., Ekanayake, S., Goode, B.J., Korkmaz, G., Kuhlman, C.J., Machi, D., Marathe, M.V., Ramakrishnan, N., Ravi, S.S., Sarat, P., Selt, N., Contractor, N., Epstein, J. and Macy, M.W. (2018). *Generative Modeling of Human Behavior and Social Interactions Using Abductive Analysis*. [online] IEEE Xplore. doi:https://doi.org/10.1109/ASONAM.2018.8508282.

Rizvi, M. (2023). Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention. 10(5), pp.055–060. doi:https://doi.org/10.22161/ijaers.105.8.

Rizvi, S.S., Bolish, T.A. and Pfeffer, J.R. (2017). Security evaluation of cloud service providers using third party auditors. doi:https://doi.org/10.1145/3018896.3025154.

Robatto Simard, S., Gamache, M. and Doyon-Poulin, P., 2023. Current Practices for Preventive Maintenance and Expectations for Predictive Maintenance in East-Canadian Mines. *Mining*, *3*(1), pp.26-53.

Rogers EM (2003) Diffusion of innovations, 5th edn. Simon and Schuster, New York, NY, USA

Salahdine, F. and Kaabouch, N., 2019. Social engineering attacks: A survey. *Future internet*, *11*(4), p.89.

Saleem, T.J. and Chishti, M.A., 2019. Data analytics in the Internet of Things: a survey. *Scalable Computing: Practice and Experience*, *20*(4), pp.607-630.

Salloum, S., Gaber, T., Vadera, S. and Shaalan, K. (2022). A Systematic Literature Review on Phishing Email Detection Using Natural Language Processing Techniques. *IEEE Access*, 10, pp.65703–65727. doi:https://doi.org/10.1109/access.2022.3183083.

Sarhan, A.Y. (2023). A novel smart multilevel security approach for secure data outsourcing in crisis. *PeerJ Computer Science*, [online] 9, p.e1367. doi:https://doi.org/10.7717/peerj-cs.1367.

Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K.-K.R. and Burnap, P. (2020). Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses. *Electronics,* 9(9), p.1460.

Sharma, N. & Garg, P., 2011. *Security Policies in Modern Database System*.

Sharma, L.R., Bidari, S., Bidari, D., Neupane, S. and Sapkota, R., 2023. Exploring the Mixed Methods Research Design: Types, Purposes, Strengths, Challenges, and Criticisms. *Glob Acad J Linguist Lit*, *5*.

Shen, B., 2023. A Survey of Access Control Misconfiguration Detection Techniques. *arXiv preprint arXiv:2304.07704*.

Shukla, A., Katt, B., Nweke, L.O., Yeng, P.K. and Weldehawaryat, G.K. (2022). System security assurance: A systematic literature review. *Computer Science Review*, 45, p.100496. doi:https://doi.org/10.1016/j.cosrev.2022.100496.

Simukali, C., Phiri, J. & Namukolo, S., 2019. *Multi Factor Authentication for Student and Staff Access Control.*

South African Industry Association, 2019. *The economic contribution of the downstream oil industry to South Africa in 2019 South African Petroleum Industry Association (SAPIA).*

Srinivas, J., Das, A.K. and Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, [online] 92, pp.178–188. doi:https://doi.org/10.1016/j.future.2018.09.063.

Stanek, M. (2017). *Secure by default -the case of TLS*. [online] Available at: https://arxiv.org/pdf/1708.07569.pdf.

Steinmetz, K.F., 2022. The identification of a model victim for social engineering: a qualitative analysis. In *The New Technology of Financial Crime* (pp. 213-237). Routledge.

Stergiopoulos, G., Gritzalis, D.A. and Limnaios, E., 2020. Cyber-attacks on the Oil & Gas sector: A survey on incident assessment and attack patterns. *IEEE Access*, *8*, pp.128440-128475.

Stewart, R. (2022). Designing Research. *Oxford University Press eBooks*, [online] pp.114–127. doi:https://doi.org/10.1093/oso/9780192868657.003.0010.

Surendran, P., 2012. *Technology Acceptance Model: A Survey of Literature.*

Tawalbeh, L.A., Muheidat, F., Tawalbeh, M. and Quwaider, M., 2020. IoT Privacy and security: Challenges and solutions. *Applied Sciences*, *10*(12), p.4102.

Tian, Y. and Nogales, A.F.R., 2023, March. A Survey on Data Integrity Attacks and DDoS Attacks in Cloud Computing. In *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 0788-0794). IEEE.

Thapa, C. and Camtepe, S., 2021. Precision health data: Requirements, challenges and existing techniques for data security and privacy. *Computers in biology and medicine*, *129*, p.104130.

Uchendu, B., Nurse, J. R. C., Bada, M. & Furnell, S., 2021. *Developing a cyber security culture: Current practices and future needs.*

Van Haute, E., 2021. SAMPLING TECHNIQUES. *Research Methods in the Social Sciences: an AZ of Key Concepts*, p.247.

Vidyasagar, S. and Murugan, A., 2021. A Study on Security Services and Threats in Cloud Computing. *Annals of the Romanian Society for Cell Biology*, pp.180-192.

Viegas, V. & Kuyucu, O., 2022. *IT Security Controls.*

Vladimir Yu. Turchaninov, Kosenkov, S.O., Oleg Samovarov, Tchij, O.P., Iakov Korovin and Schaefer, G. (2018). High-Performance Cloud Computing for Managing the Life Cycle of Oil and Gas Fields. *Advances in intelligent systems and computing*. doi:https://doi.org/10.1007/978-981-10-8944-2_127.

Wanasinghe, T.R., Gosine, R.G., James, L.A., Mann, G.K., De Silva, O. and Warrian, P.J., 2020. The internet of things in the oil and gas industry: a systematic review. *IEEE Internet of Things Journal*, *7*(9), pp.8654-8673.

Wang, Z. and Chen, L., 2020, December. Re-encrypted data access control scheme based on blockchain. In *2020 IEEE 6th International Conference on Computer and Communications (ICCC)* (pp. 1757-1764).

Warikandwa, T.V. (2021). Personal Data Security in South Africa's Financial Services Market: The Protection of Personal Information Act 4 of 2013 and the European Union General Data Protection Regulation Compared. *Potchefstroom Electronic Law Journal*, [online] 24, pp.1–32. doi:https://doi.org/10.17159/1727-3781/2021/v24i0a10727.

Whitehead, G. (2020). *Investigation of factors influencing cybersecurity decision making in Irish SME's from a senior manager/owner perspective*.

Wijesundara, WMAB, Lee, J.-S., Tith, D., Aloupogianni, E., Suzuki, H. and Obi, T. (2023). Security-enhanced firmware management scheme for smart home IoT devices using distributed ledger technologies. [online] doi:https://doi.org/10.21203/rs.3.rs-3077169/v1.

Williamson, J. and Curran, K. (2021). Best Practice in Multi-factor Authentication. *Semiconductor Science and Information Devices*, 3(1). doi:https://doi.org/10.30564/ssid.v3i1.3152.

Wilson, D. A., 2018. *Accepting The Future: Comparing The Adoption Of Technology By Age Cohorts*

Worthington, A.K. and Burgess, G.L. (2021). Technology Acceptance Model. *ua.pressbooks.pub*. [online] Available at: https://ua.pressbooks.pub/persuasiontheoryinaction/chapter/technology-acceptance-model/.

Yildirim, M. (2021). *Artificial Intelligence-Based Solutions for Cyber Security Problems*. [online] Artificial Intelligence Paradigms for Smart Cyber-Physical Systems. Available at: https://www.igi-global.com/chapter/artificial-intelligence-based-solutions-for-cyber-security-problems/266133.

Yıldırım, M. and Mackie, I. (2019). Encouraging users to improve password security and memorability. *International Journal of Information Security*, [online] 18(6), pp.741–759. doi:https://doi.org/10.1007/s10207-019-00429-y.

Zamir, H., 2020. Cybersecurity and Social Media. *Cybersecurity for Information Professionals: Concepts and Applications*, p.153.

Zheng, Y., Li, Z., Xu, X. and Zhao, Q., 2022. Dynamic defenses in cyber security: Techniques, methods and challenges. *Digital Communications and Networks*, *8*(4), pp.422-435.

Zhifeng, Y., Xuehui, F., Fei, H., Qi, Y., Zhen, C. and Yidan, Z., 2019. Cloud computing and big data for oil and gas industry application in China.

# ANNEXURES

## Annexure A: Consent to Participate in Study

**Faculty of Business and Management Sciences**
**Ethics Informed Consent Form**

**CONSENT TO PARTICIPATE IN A RESEARCH STUDY**

**Category of Participants (tick as appropriate):**

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| *Staff/Workers* | *X* | *Teachers* | | *Parents* | | *Lecturers* | | *Students* | |
| *Other (specify)* | | | | | | | | | |

You are kindly invited to participate in a research study being conducted by Zandiswa Nkandi from the Cape Peninsula University of Technology. The findings of this study will contribute towards the *Master's thesis*.

The tittle of the research study being conducted is "***An awareness model for the use of information technology security policies in the petroleum retail sector in South Africa"*** and the main objective of this study is to develop an awareness model for the use of IT security compliance policies in the petroleum retail sector. This research is important to assist the petroleum retail sector protect its information from cybersecurity threats and realise its full potential in terms of IT security policy compliance.

Your participation in this research study is voluntary and no compensation will be provided for your involvement. Participants' names and organisation names will not be disclosed or published as part of this study; anonymity and confidentiality will be maintained.

The method of data collection will consist of a questionnaire, which will take approximately 10 to 15 minutes to complete.

Should you have any questions regarding this study, please contact:

- The researcher, Zandiswa Nkandi at 0784060137 or zandinkandi@gmail.com.
- The research supervisor, Ephias Ruhode at 0728026329 or RuhodeE@cput.ac.za.

Kindly complete the table below before participating in the research.

| **Tick the appropriate column with an X** | | |
|---|---|---|
| **Statement** | Yes | No |
| 1. I understand the purpose of the research. | x | |
| 2. I understand what the research requires of me. | x | |
| 3. I volunteer to take part in the research. | x | |
| 4. I know that I can withdraw at any time. | x | |
| 5. I understand that there will not be any form of discrimination against me as a result of my participation or non-participation. | x | |

Please only provide signature on the block provided below and return the signed document at your earliest convenience. You will be given a copy of this form on request.

| | |
|---|---|
| Signature of participant: | Date: |

**Annexure B: Introductory Letter for Collection of Data**

**Introductory letter for the collection of research data**

*Zandiswa Nkandi* is registered for the *Masters in Information Technology at CPUT (204126827)*. The thesis is titled *An awareness model for the use of information technology security policies in the petroleum retail sector in South Africa* and aims *to develop an awareness model for the use of IT security compliance policies in the petroleum retail sector.* The supervisor(s) for this research is/are:

*Prof Ephias Ruhode - 0728026329*

In order to meet the requirements of the university's Higher Degrees Committee (HDC) the student must get consent to collect data from individuals and organisations which they have identified as potential sources of data. In this case, the student will use *one-on-one virtual interviews which will last approximately 30 to 40 minutes* to gather data.

If you agree to this, you are requested to complete the attached form (an electronic version can be made available to you) and print it on your organisation's letterhead (where possible).

Please note that no data will be gathered until the researcher has received ethics clearance from CPUT.

For further clarification on this matter, please contact either the supervisor(s) identified above, or the Faculty Research Ethics Committee secretary (Mziyanda Ndede) at 021 469 1014 or ndedem@cput.ac.za

Yours sincerely

*Ephias Ruhode*

*27/11/2022*

## Annexure C: Letter of Consent -Engen

With us you are Number One | ENGEN

I *Aveena Mothilall,* in my capacity as *Chief Information Officer* at *Engen Petroleum* give consent in principle to allow *Zandiswa Nkandi,* a student at the Cape Peninsula University of Technology, to collect data in this company/from me as part of their *master's in information technology* research. The student has explained to me the nature of their research and the nature of the data to be collected.

This consent in no way commits any individual person to participate in the research, and it is expected that the student will get individual consent from any participants. I reserve the right to withdraw this permission at any time.

In addition, the company's/my name may or may not be used as indicated below (tick as appropriate):

| | Thesis | Conference paper | Journal article | Research poster |
|---|---|---|---|---|
| **Yes** | | | | |
| **No** | X | X | X | X |

Aveena Mothilall - CIO Engen Petroleum

28 November 2022

## Annexure D: Ethical Clearance

Cape Peninsula University of Technology
creating futures

PO Box 1906, Bellville,7535 Symphony Way, Bellville, Cape Town, South Africa
+ 27 (0)21 959 6767 www.facebook.com/cput.ac.za info@cput.ac.za www.cput.ac.za

**Office of the Research Ethics Committee**
Faculty of Informatics and Design
Room 2.09
80 Roeland Street
Cape Town
**Tel: 021-469 1012**
**Email: ndedem@cput.ac.za**
**Secretary: Mziyanda Ndede**

22 February 2023

Mrs Zandiswa Nkandi
c/o Department of Information Technology
CPUT

**Reference no:** 204126827/2023/4

**Project title:** An awareness model for the use of information technology security policies in the petroleum retail sector in South Africa

**Approval period:** 22 February 2023 – 31 December 2024

This is to certify that the Faculty of Informatics and Design Research Ethics Committee of the Cape Peninsula University of Technology approved the methodology and ethics of Mrs Zandiswa Nkandi (204126827) for Master of Information Technology.

Any amendments, extension or other modifications to the protocol must be submitted to the Research Ethics Committee for approval.

The Committee must be informed of any serious adverse event and/or termination of the study.

**Dr Blessing Makwambeni**
**Acting Chair: Research Ethics Committee**
**Faculty of Informatics and Design**
**Cape Peninsula University of Technology**

## Annexure E: Interview Questionnaire

| INTERVIEW QUESTIONNAIRE | | | | | |
|---|---|---|---|---|---|
| 1. The password policy is available and easily accessible to me. | ☐ Strongly Agree | ☐ Agree | ☐ Disagree | ☐ Strongly Disagree | ☐ I don't know |
| 2. Utilising strong and not easy to guess passwords is essential to protect me from cyber-attacks. | ☐ Strongly Agree | ☐ Agree | ☐ Disagree | ☐ Strongly Disagree | ☐ I don't know |
| 3. I frequently utilise a Virtual Private Network (VPN) in my day-to-day activities. | ☐ Strongly Agree | ☐ Agree | ☐ Disagree | ☐ Strongly Disagree | ☐ I don't know |
| 4. VPN is easy to use, in my opinion. | ☐ Strongly Agree | ☐ Agree | ☐ Disagree | ☐ Strongly Disagree | ☐ I don't know |
| 5. My work computer provides the capability to connect and utilise a personal USB storage device. | ☐ Strongly Agree | ☐ Agree | ☐ Disagree | ☐ Strongly Disagree | ☐ I don't know |
| 6. I utilise social media platforms, including WhatsApp, Telegram, Facebook, and Instagram, as channels for sharing organisational data. | ☐ Strongly Agree | ☐ Agree | ☐ Disagree | ☐ Strongly Disagree | ☐ I don't know |
| 7. Within the past six months, I have participated in online or in-person training sessions that focused on cybersecurity. | ☐ Strongly Agree | ☐ Agree | ☐ Disagree | ☐ Strongly Disagree | ☐ I don't know |
| 8. Within my organisation, I have access to a training platform that offers cybersecurity-related training topics. | ☐ Strongly Agree | ☐ Agree | ☐ Disagree | ☐ Strongly Disagree | ☐ I don't know |
| 9. I have the capability to use my personal computer to gain access to organisational data and applications. | ☐ Strongly Agree | ☐ Agree | ☐ Disagree | ☐ Strongly Disagree | ☐ I don't know |
| 10. I have the capability to use my work computer to access personal data and applications. | ☐ Strongly Agree | ☐ Agree | ☐ Disagree | ☐ Strongly Disagree | ☐ I don't know |
| 11. I use my personal device to access organisational sensitive or personal information (POPIA / confidential). | ☐ Strongly Agree | ☐ Agree | ☐ Disagree | ☐ Strongly Disagree | ☐ I don't know |
| 12. Occasionally, I use public **spaces** (airplane/airport, hotel, restaurant) to access confidential data or information while traveling or working remotely. | ☐ Strongly Agree | ☐ Agree | ☐ Disagree | ☐ Strongly Disagree | ☐ I don't know |
| 13. Occasionally, I connect to public **Wi-Fi** (airport, hotel, restaurant) to access confidential data or information while traveling or working remotely. | ☐ Strongly Agree | ☐ Agree | ☐ Disagree | ☐ Strongly Disagree | ☐ I don't know |
| 14. I regularly share organisational information or data with partners, contractors, customers, suppliers, or vendors. | ☐ Strongly Agree | ☐ Agree | ☐ Disagree | ☐ Strongly Disagree | ☐ I don't know |
| 15. I understand what is expected of me from the cybersecurity perspective. | ☐ Strongly Agree | ☐ Agree | ☐ Disagree | ☐ Strongly Disagree | ☐ I don't know |
| 16. I know where to find information about cybersecurity. | ☐ Strongly Agree | ☐ Agree | ☐ Disagree | ☐ Strongly Disagree | ☐ I don't know |
| 17. I know where to report cybersecurity related questions. | ☐ Strongly Agree | ☐ Agree | ☐ Disagree | ☐ Strongly Disagree | ☐ I don't know |
| 18. I understand security capabilities around my home network / Wi-Fi. | ☐ Strongly Agree | ☐ Agree | ☐ Disagree | ☐ Strongly Disagree | ☐ I don't know |

| | | | | | |
|---|---|---|---|---|---|
| 19. I understand my responsibility / obligation to log all security related incidents. | ☐ Strongly Agree | ☐ Agree | ☐ Disagree | ☐ Strongly Disagree | ☐ I don't know |
| 20. Cybercriminals or scammers have previously attempted to carry out a cyberattack against my work computer. | ☐ Strongly Agree | ☐ Agree | ☐ Disagree | ☐ Strongly Disagree | ☐ I don't know |
| 21. My work computer has been successfully hacked or exploited in the past. | ☐ Strongly Agree | ☐ Agree | ☐ Disagree | ☐ Strongly Disagree | ☐ I don't know |
| 22. The computer provided by my organisation grants me access to various social media platforms. | ☐ Strongly Agree | ☐ Agree | ☐ Disagree | ☐ Strongly Disagree | ☐ I don't know |
| 23. What is the frequency at which your organisation provides cybersecurity training? | ☐ Yearly | ☐ Quarterly | ☐ Monthly | ☐ Never | ☐ I don't know |
| 24. What do you do if you suspect an email has been phished or if you spot any non-compliance concerns? | ☐ Report to line manager | ☐ Report via Phish alert | ☐ Report to Service Desk | ☐ I do nothing | ☐ I don't know |
| 25. Which MFA or two-factor authentication method do you find best to use usage? | ☐ Authenticator App | ☐ SMS code | ☐ Phone call | ☐ I don't know | ☐ I don't know |
| 26. In terms of cybersecurity policies and awareness, what is your level of understanding? | ☐ I understand fully | ☐ I understand | ☐ Neutral | ☐ I don't understand | ☐ I don't know |
| 27. Is there anything in particular that you think contributes to employees falling victim of cyber-attack within an organisation? Please provide details in the space provided below: | | | | | |
| | | | | | |

**Annexure F: Interview Questionnaire Draft**

**INTERVIEW QUESTIONNAIRE DRAFT**

| |
|---|
| **Technology** |
| 1. Utilizing strong and not easy to guess passwords is essential to protect me from cyber-attacks. |
| 2. I frequently utilize a Virtual Private Network (VPN) in my day-to-day activities. |
| 3. VPN is easy to use, in my opinion. |
| 4. My work computer provides the capability to connect and utilize a personal USB storage device. |
| 5. I have the capability to use my personal computer to gain access to organizational data and applications. |
| 6. I have the capability to use my work computer to access personal data and applications. |
| 7. I use my personal device to access organizational sensitive or personal information (POPIA / confidential). |
| 8. Occasionally, I use public **spaces** (airplane/airport, hotel, restaurant) to access confidential data or information while traveling or working remotely. |
| 9. Occasionally, I connect to public **Wi-Fi** (airport, hotel, restaurant) to access confidential data or information while traveling or working remotely. |
| 10. I know where to report cybersecurity related questions. |
| 11. I understand security capabilities around my home network / Wi-Fi. |
| 12. I understand my responsibility / obligation to log all security related incidents. |
| 13. The computer provided by my organization grants me access to various social media platforms |
| 14. What do you do if you suspect an email has been phished or if you spot any non-compliance concerns? |
| 15. Which MFA or two-factor authentication method do you find best to use usage? |
| **Organisation** |
| 16. Within my organization, I have access to a training platform that offers cybersecurity-related training topics. |
| 17. Within the past six months, I have participated in online or in-person training sessions that focused on cybersecurity. |
| 18. I utilize social media platforms, including WhatsApp, Telegram, Facebook, and Instagram, as channels for sharing organizational data. |
| 19. I understand what is expected of me from the cybersecurity perspective. |
| 20. I know where to find information about cybersecurity. |
| 21. The password policy is available and easily accessible to me. |
| 22. What is the frequency at which your organization provides cybersecurity training? |
| 23. In terms of cybersecurity policies and awareness, what is your level of understanding? |
| **Environment** |
| 24. I regularly share organisational information or data with partners, contractors, customers, suppliers, or vendors. |
| 25. Cybercriminals or scammers have previously attempted to carry out a cyberattack against my work computer. |
| 26. My work computer has been successfully hacked or exploited in the past. |