

https://dspace.org/

Strategies to mitigate ransomware related cyber-attacks in South African financial institutions

Mahlangu, Nqobile

2023
University of the Witwatersrand, Johannesburg
https://hdl.handle.net/10539/43933
Mahlangu, Nqobile. (2023). Strategies to mitigate ransomware related cyber-attacks in South African financial institutions[Master's dissertation, University of the Witwatersrand, Johannesburg].WireDSpace.

Downloaded from a DSpace repository. https://dspace.org/

Strategies to mitigate ransomware related cyber-attacks in South African financial institutions

Nqobile Mahlangu

2159255

A research report submitted to the Faculty of Commerce, Law and Management, University of the Witwatersrand, in partial fulfilment of the requirements for the degree of Master of Management in the field of Digital Business

Johannesburg, 2023

ABSTRACT

Digital transformation has become topical amongst many organisations and industries alike. Inherent to the adoption of technology to optimise business processes and operations, cyber-attacks have become a growing concern, with ransomware becoming a top concern for organisations. South African banks have not been immune to the associated ransomware risks, as threat actors continue to find motivation to attempt infiltrating SA banks, compromising their confidentiality, integrity, and availability thereafter and demanding a ransom.

Cyber-resilience is positioned as an attractive strategy to prevent and mitigate ransomware attacks. This study investigates the effectiveness of employing a cyber-resilience strategy in mitigating ransomware attacks within South African financial institutions, in particular SA banks. The study explores various best practices and factors that influence cyber-resiliency, the role that management plays in ensuring cyber-resiliency, and finally, various methods that can be employed to assess the effectiveness of cyber-resilience as a strategy.

The study employs a qualitative research approach, using semi-structured interviews to collect data. With the permission granted by participants, all interviews were recorded, transcribed, and then analysed using thematic analysis.

The research questions, which delve into the outlined research objectives, serve as a guide for the discussions of the findings. Literature and findings from the study show that ransomware is considered a top concern for SA banks, with an agreement that “it is not a matter of if ransomware attacks will happen, but rather a matter of when.” In response to this, findings show that the organisations covered in the scope of the study have employed a cyber-resilience strategy for prevention and mitigation of ransomware attacks, as it is noted as an effective strategy in preventing and mitigating ransomware attacks.

KEYWORDS

Cyber-attacks, ransomware, threat actors, Denial-of-service, cyber resilience, financial institutions, exposure, cyber-crime, NIST Framework, cyber threats

DECLARATION

I, Nqobile Mahlangu attest that this research report is created using my own knowledge, investigation, and use of the materials and sources cited in the report. The report is submitted in partial fulfilment of the requirements for the degree of Master of Management in the field of Digital Business at the University of the Witwatersrand, Johannesburg. This research paper has not been submitted for a degree or an exam at another university in the past.

Name: Nqobile Mahlangu **Signature:** 

Date: 28 September 2023

DEDICATION

This research paper is dedicated to my darling husband Felane Mahlangu, my son Lethumusa and daughter Zenokuhle; it is through your love, patience, prayers, and encouragement that I was able to complete this paper. I love and appreciate you always.

ACKNOWLEDGEMENTS

First, I would like to raise up my praises in gratitude to my Lord and saviour Jesus Christ, for through Him I was able to successfully complete this paper.

To my wonderful husband, Felane for the encouragement, patience, prayers and holding me accountable throughout this journey. Thank you for always understanding and accommodating me, your unwavering support is not taken for granted and is credited to me succeeding in the completion of this paper.
To my two beautiful children, Lethumusa and Zenokuhle for your patience and understanding, giving up some of your play time with mom so I can focus on completing this paper.

To my family and friends, with a special mention of my mom, dad and 'mama Thoko,' thank you for your continued support and words of encouragement throughout this journey.

To my supervisor, Dr Kiru Pillay for the patience through the various challenges, the support, guidance, and valuable knowledge shared throughout this journey.

To my employer and funder, for availing and encouraging learning opportunities, for your support and understanding throughout the process of completing this research project.
Lastly, I would like to thank all the participants for availing themselves and partake in the study, the insights provided, and valuable discussions have contributed immensely towards the success of this paper.

TABLE OF CONTENTS

ABSTRACT ii

DECLARATION iii

DEDICATION iv

ACKNOWLEDGEMENTS v

LIST OF FIGURES x

LIST OF TABLES xii

LIST OF ACRONYMS xiii

1 Introduction 15

1.1 STATEMENT OF PURPOSE 15

1.2 BACKGROUND OF THE STUDY 15

1.2.1 FINANCES SERVICES 15

1.2.2 THREATS 16

1.2.3 RANSOMWARE 16

1.2.4 CYBER-RESILIENCE 19

1.3 RESEARCH PROBLEM 22

1.4 RESEARCH OBJECTIVES 22

1.5 RATIONALE 23

1.6 DELIMITATIONS OF THE STUDY 24

1.7 ASSUMPTIONS 24

1.8 DEFINITION OF TERMS 25

1.9 CHAPTER OUTLINE 26

2 Literature Review 28

2.1 INTRODUCTION 28

2.2 CYBER THREATS 28

2.2.1 CYBER THREAT LANDSCAPE 28

2.2.2 CYBER-ATTACKS ON FINANCIAL INSTITUTIONS 32

2.3 RANSOMWARE 36

2.3.1 ORIGINS OF RANSOMWARE? 36

2.3.2 CATEGORIES OF RANSOMWARE? 38

2.3.3 GLOBAL TRENDS OF RANSOMWARE 38

2.3.4 IMPACT OF RANSOMWARE ON SOUTH AFRICAN BANKING SECTOR 39

2.4 CYBER RESILIENCE 42

2.4.1 Defining Cyber Resilience 42
2.4.2 Understanding Cyber Resilience as a strategy 42
2.5 Frameworks and best practices that inform cyber resilience 45
2.5.1 ISO 27000 Series 46
2.5.2 NIST Cybersecurity Framework 46
2.5.3 COBIT 48
2.6 Evaluation methods of cyber-resilience 49
2.6.1 Cyber Resilience Review (CRR) 50
2.6.2 Cyber-resilience assessment framework (C-RAF) 51
2.6.3 Assurance Reviews 54
2.6.4 Metrics 55
2.7 Senior Management and Cyber resiliency 57
2.7.1 Management's awareness of ransomware as a top risk 57
2.7.2 Role of senior management in ensuring cyber-resilience 57
2.8 Analytical Framework 59
2.8.1 Theoretical Framework 59
2.8.2 NIST Framework 62
2.9 Conceptual Framework 68
2.10 Research Propositions 65
2.10.1 Proposition 1 65
2.10.2 Proposition 2 65
2.10.3 Proposition 3 65
2.10.4 Proposition 4 66
2.11 Conclusion: 66

3 Research Methodology 68

3.1 Research approach 68
3.2 Research design 70
3.3 Data Collection Methods 71
3.4 Population and sample 71
3.4.1 Population 71
3.4.2 Sample 72
3.4.3 Sampling method 72
3.5 The Research Instrument 73
3.6 Procedure for data collection 73
3.7 Data analysis and interpretation 75
3.8 Limitations of the study 77
3.9 Quality Assurance 78
3.9.1 Credibility 78
3.9.2 Dependability 80
3.9.3 Triangulation 80
3.10 Demographic profile of respondents 82
3.11 Ethical considerations 82
3.12 Conclusion 83

4 Research Findings 85

4.1 Introduction 85

4.2 Research objective 1: Assess the level of concern and prioritization that organisations have on ransomware cyber-attacks; 87

4.3 Research objective 2: Investigate the key influences that contribute to a cyber-resilient posture of an organisation against ransomware attacks; 89

4.4 Research objective 3: Assess the role and influence of senior management in influencing the resilient posture against ransomware cyber-attacks; 92

4.5 Research objective 4: Investigate how organisations can evaluate the effectiveness of cyber resilience as a mitigating strategy; 96

4.6 Summary of findings 98

5 Discussion of findings 103

5.1 Introduction 103

5.2 Discussion on assessing the level of concern and prioritization that organisations have on ransomware cyber-attacks; 103

5.2.1 Discussion on the investigation of the key influences that contribute to a cyber-resilient posture of an organisation against ransomware attacks; 105

5.2.2 The ability to identify 105

5.2.3 Ability to protect 106

5.2.4 Ability to respond and recover 107

5.3 Role of Senior Management 108

5.3.1 Prioritizing Cyber-resilience 109

5.3.2 Encouraging a cyber-resilient culture 109

5.3.3 Discussion on the evaluation of cyber-resilience 110

5.3.4 Benchmarking against industry standards 110

5.3.5 Red Teaming Exercises and Penetration Tests 111

5.3.6 Tabletop and Simulation Exercises 112

5.3.7 Backup, DR and Restoration Testing 112

5.3.8 Use of Metrics 113

5.4 Conclusion 113

6 Conclusions and Recommendations 114

6.1 Introduction 114

6.2 Conclusion regarding RQ1 114

6.3 Conclusion regarding RQ2 115

6.4 Conclusion regarding RQ3 115

6.5 Conclusion regarding RQ4 116

6.6 Recommendations 116

6.7 Suggestions for further research 117

7 REFERENCES _____ **118**

APPENDIX A: Information sheet _____ **124**

APPENDIX B: Agreement form _____ **126**

APPENDIX C: Interview guide _____ **127**

APPENDIX D: Research analysis data association _____ **130**

APPENDIX E: Ethical Clearance Certificate _____ **134**

LIST OF FIGURES

Figure 1 Cyber-kill Chain Model (Source: Researcher, 2023) 18

Figure 2 How a Botnet Attack Works (Source: BasuMallick (2022)) 30

Figure 3 The flow of ransomware works (Source: Leventopoulos (2022)) 32

Figure 4 Number of cyber incidents in the financial industry worldwide from 2013 to 2021 (Source: Petrosyan (2022) 33

Figure 5 Evolution of Ransomware (Source: O'Kane et al, 2018) 37

Figure 6 Categories of ransomware (Andronio et al., 2015)..... 38

Figure 7 Ransomware by the numbers (Source: (MARSH, 2023)..... 39

Figure 8 The Cyber Resilience Process (Source: Conklin et al. (2017)) .....**Error! Bookmark not defined.**

Figure 9 Five Principles of COBIT 5 (Source: IT Governance (2022)) .....**Error! Bookmark not defined.**

Figure 10 CRR Domain Composition (Source: U.S. Department of Homeland Security (2020))..... 51

Figure 11 Inherent Risk Rating mapping to Expected Maturity Level (Source: Lee (2016)) 52

Figure 12 Maturity assessment (in seven domains). (Source: Lee (2016)) 53

Figure 13 Components of the maturity assessment (Source: Hong Kong Monetary Authority, 2016)..... 54

Figure 14 Cyber Resiliency Metrics Can Repurpose Security, Risk, or Resilience Metrics (Source: Bodeau et al., (2018)) 56

Figure 15 Routine Activity Theory (RAT) (Source: Govender et al., (2021) 60

Figure 16 Application of Routine Activity Theory (Researcher own, 2022) 62

Figure 17 Five Core functions for effective Cybersecurity (Source: Hanacek, 2018)..... 63

Figure 18 Adaptive Cyber Resilient Framework (Researcher own, 2023)..... 69

LIST OF TABLES

Table 1 Cyber incidents involving financial institutions (Source: (Carnegie, 2023) 36

Table 2 Cyber incidents involving financial institutions (Source: (Carnegie, 2023) 42

Table 3 Common Assurance Methods (Source: National Cyber Security Centre (2023)..... 55

Table 4 Types of Triangulation (Source: Guion (2002)) 81

Table 5 Information of participants 86

LIST OF ACRONYMS

APT: Advanced Persistent Threats

CIA: Confidentiality, Integrity, and Availability

CIO: Chief Information Officer

CISO: Chief Information Security Officer

COBIT: Control Objectives for Information and Related Technologies

CRMM: Cyber Resilience Maturity Model

CRR: Cyber Resilience Review

CSIR: Council for Scientific and Industrial Research

DDOS: Distributed Denial of Service

DLP: Data Loss Prevention

ICT: Information and Communication Technology

IDS: Intrusion Detection System

IPS: Intrusion Prevention System

IRP: Incident Response Plan

ISO/IEC: International Organisations for Standardisation/ International Electrotechnical Commission

ISS: Information Systems Security

NCPF: National Cybersecurity Policy Framework

NIST: National Institute of Standards and Technology

RAT: Routine Activity Theory

SA: South Africa

SABRIC: South African Banking and Risk Information Centre

VA: Vulnerability Assessment

1 Introduction

1.1 Statement of purpose

This qualitative study investigates the effectiveness of cyber-resilience as a strategy in mitigating ransomware cyber-attacks within the South African financial sector.

1.2 Background of the study

In recent years, digital transformation has become topical as many organisations in both the public and private sectors have explored ways to use technology to digitally reach their customers, automate their processes, and leverage the data generated to develop various efficiencies and remain competitive (Blafka, 2023). The drive for digital transformation within organisations can be linked to the rapid and prominent introduction of digital innovations, which are causing what is termed 'digital disruption' across different industries (Skog, Wimelius, & Sandberg, 2018).

Bradley et al. (2015) introduces the concept of a digital vortex to highlight how various industries are impacted by digital disruptions. The digital vortex illustrates the inevitable movement of the different industries towards a "digital centre," where digitization of processes, business offerings, customer reach are to be digitised.

1.2.1 Finances Services

One of the industries identified as being drawn into the centre of the digital vortex is financial services. 'Financial Services' cover a broad range of activities, which include banking, investing, and insurance (Asmundson, 2011). In considering the role that financial services play in a South African context, the National Treasury Policy Document (2011) describes financial services as being at the heart of the South African economy, which allows people to make daily economic transactions, save and preserve wealth to meet future aspirations and retirement needs, and insure against personal disaster. The Treasury report (2011) further

highlights that financial services “enable economic growth, job creation, the building of vital infrastructure, and sustainable development for South Africa”.

As financial services digitally transform and adopt technologies that enable their strategic objectives, they also become inherently more vulnerable to cyber-attacks. According to Pieterse (2021), the frequency and severity of cyber-attacks have escalated and have been experienced on a global scale. South Africa has not been immune to these cyber-attacks.

1.2.2 Threats

Cyberattacks have increased, particularly in South Africa, according to a Surfshark report that places the country among the top five nations affected by cybercrime and shows that the country's cybercrime density increased by 7.8% between 2021 and 2022 (DefenceWeb, 2023).

According to a report by Accenture (2020), South Africa was highlighted as “having the third most cybercrime victims worldwide, causing a loss of R2,2 billion a year”. The rise in cyber threats is indicating that cyber criminals are finding South Africa an attractive target. The Accenture report (2020) further argues that threat actors perceive South African organisations to have lower defences as compared to developed countries, together with a widely spread belief that one has a lower chance of being caught or prosecuted if committing a crime in South Africa. The following are enlisted as interconnected factors that contribute to threat actors targeting South Africa:

- Lack of investment in cybersecurity
- Developing cybercrime legislation and law enforcement training
- Poor public knowledge of cyber threats
- The use of shadow IT

1.2.3 Ransomware

While there are a number of cyber-attack vectors used by threat actors, the use of ransomware as an attack path has increased in popularity. Ransomware is

understood as ‘a form of malware that uses algorithms to encrypt a user’s files so that they cannot be accessed without a decryption key.’ The attackers then request that an amount of money commonly used in cryptocurrency be paid to them in exchange for the decryption key (Group IB, 2018). It is important to note that the deployment of ransomware is the last step of a successful attack, after which a threat actor would have successfully breached the network of an organisation, stole, and/or further proceeded to encrypt the data. To understand the key phases threat actors follow to successfully deploy a ransomware attack, one can consider the Cyber Kill Chain model with an example attack path as illustrated in Figure.1.1 below:

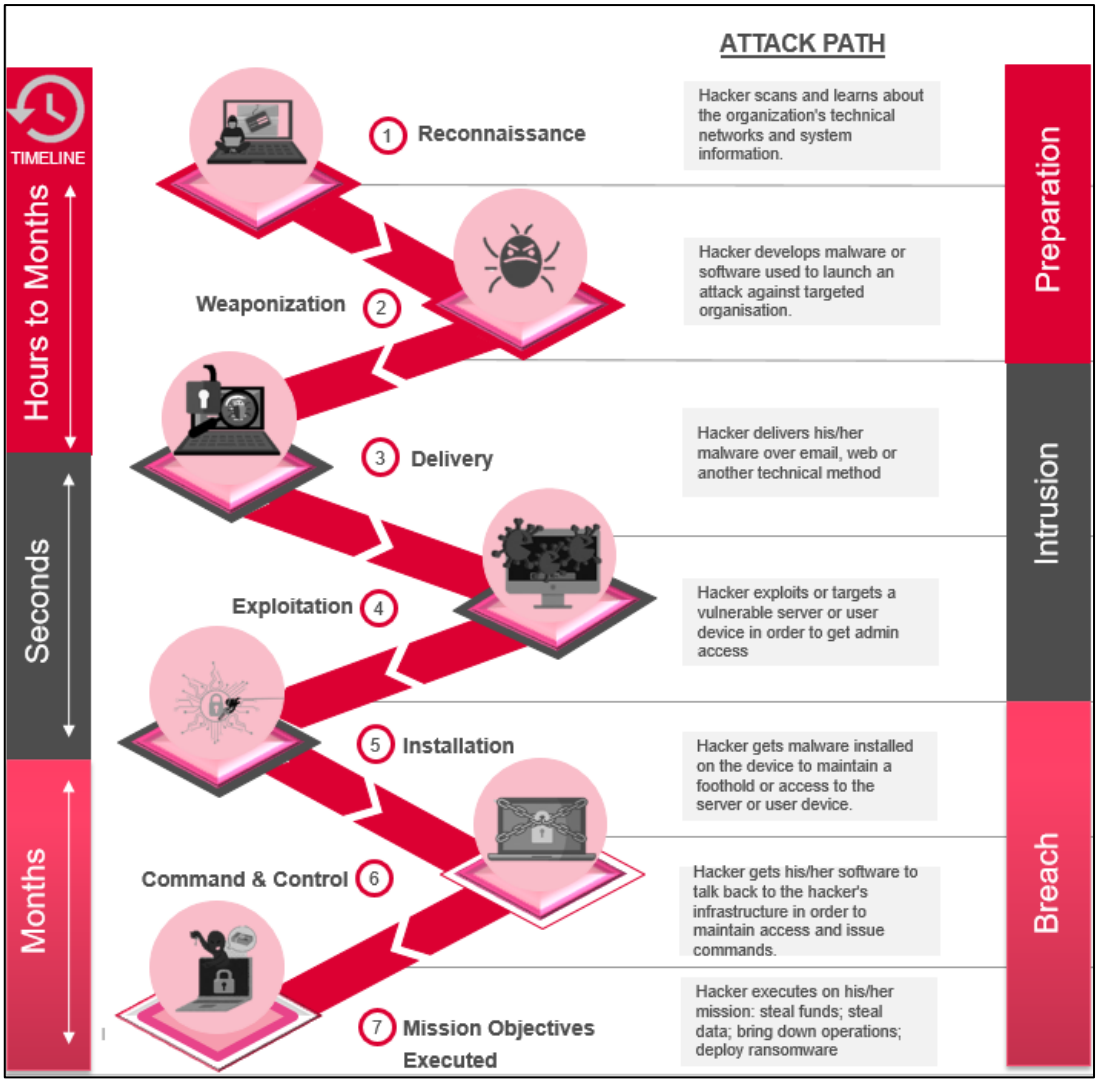


Figure 1 Cyber-kill Chain Model (Source: Researcher, 2023)

The rise in using this attack path can be attributed to the financial gain that threat actors stand to potentially gain if successful in deploying ransomware. Additionally, the introduction of ransomware-as-a-service (RaaS) has made it easy for underground criminals to access ransomware and conduct malicious activity without needing to be highly skilled. Accenture (2020) further suggests that some threat actors use South Africa as a testing ground for malware before deploying against targets that are more sophisticated.

Ransomware attacks in South Africa remain a top-of-mind threat for many organisations, with South Africa cited as the country most affected by targeted ransomware in the first quarter of 2021, according to Interpol (2021).

Some notable ransomware attacks and attempts include the following recorded incidents:

- **2019** | South African Banking and Risk Information Centre (SABRIC) confirmed a ransom-driven Distributed Denial-of-service (DDOS) attack that targeted various South African banks (Fin24, 2019).

- **2021** | South African banks were caught up in a third-party exposure where a debt collector (Debt-IN) associated with several SA Banks was compromised by a ransomware attack, exposing as much as 1.4 million personal records of South Africans (Moyo, 2021).
- **2021** | State enterprise Transnet experienced a cyber-attack which affected container terminals and forced Transnet to halt operations at container terminals in several Cities in South Africa. Transnet was forced to declare force majeure at their container terminals and switch to manual processing of Cargo (CCDCOE, 2021).
- **2023** | The Western Cape Provincial parliament experienced a cyber-attack where for a period their ICT systems were rendered as inaccessible (McCain, 2023)

A study by the Central Bank indicates that a number of cyber threats are increasing within the banking sector, with a Prudential Authority report highlighting ransomware as an attack path also being on the rise and a concern for the South African banking sector (SARB, 2022).

In the case of financial services, when it comes to the defence, response, and recovery from cybercrimes, cyber resilience is of paramount importance, as it is critical to ensure that they can maintain the confidentiality, integrity, and availability (CIA) of the data and systems used. This is often cited as the “crown jewel," which attackers may seek to compromise.

1.2.4 Cyber-resilience

Consequently, cyber resilience, which is commonly understood as an organisation's ability to anticipate, prevent, withstand, and recover from cyber-attacks (Ross R. et al., 2021), has equally become a top priority for organisations.

Cyber resilience comprehensively relies on the key goals, which, according to Ross et al. (2021) include:

Anticipation: an organisation being able to anticipate threats, which can be achieved in several ways, such as by identifying and understanding the organisation's assets so adequate plans can be created in case a threat materializes. Investing in threat intelligence capabilities can also assist an organisation in being better prepared for potential attacks. The key driver of anticipating attacks is to ensure that an organisation can plan and potentially prevent the likelihood of an attack materialising.

Prevent: Preventative solutions may not always provide a foolproof solution to potential cyber-attacks, but they can help organisations reduce the probability of an attack taking place as well as limit an attack's blast radius. Some of the common approaches to increasing prevention include having strict access controls in place, ensuring there are backups in place, and increasing user awareness and training to build a human defence (Beaman et al., 2021).

Withstanding: Being prepared to withstand an attack assumes that an attack will happen, and when it does, the organisation would need to be clear in its response. A response to an attack takes varied forms when considering the risk appetite of the organisation. Depending on the level of potential impact, an organisation can choose to absorb some level of attack but ensure that the infection is contained to reduce the blast radius of infection throughout the network by implementing solutions like network segmentation and zero trust. Organisations can also elect to deflect and transfer the risk to an insurance company, which, in the case of ransomware, can assist in ransom payments or the recoverability of lost systems.

Recovery: Planning for a recovery means if an attack would have materialised, and losses would have been experienced by the organisation. A key factor in being able to recover is ensuring that backups are in place and that the organisation can adequately recover from those backups. In the case of ransomware, having backups that are linked to your network may prove to be futile if an attacker is able to reach and alter the backups as part of an attack. A

growing alternative is for organisations to ensure that they have immutable backups or offline copies from which they can recover. A pertinent question remains, whether organisations would be able to recover fast enough to limit business impact and maintain their CIA even if they had immutable or offline backups.

Adapt: To ensure sustainable cyber resiliency, an organisation needs to maintain continuous correction by removing or adding new controls that are fit for purpose and in line with the changing threat landscape. Through strategies of attack simulation, intelligence collected on emerging threats, or simply learning from materialised cyber-attacks, organisations can better prepare themselves by reviewing, redefining, and adjusting things like systems' requirements, architecture, design, configuration, acquisition processes, or operational processes to ensure that resiliency is maintained.

When putting together a cyber-resilience strategy, one also needs to consider cybersecurity frameworks, which would be fit for purpose as a guide. One popular framework is the National Institute of Standards and Technology (NIST) security framework, which provides guidance on what organisations need to consider as part of improving their cyber resilience (Scofield, 2016). The NIST framework is cited as a widely accepted and adopted approach by organisations to facilitate cybersecurity risk management (Gordon, Loeb, & Zhou, 2020). The NIST Cybersecurity Framework is intentionally broad and flexible to allow companies to adopt the macro-overview approach while having the flexibility to apply the details of the implementation in line with organisations' needs and strategies (Gordon, Loeb, & Zhou, 2020). The framework achieves this by outlining five main functions: identify, protect, detect, respond, and recover, giving organisations guidance on which function they may need to focus on to improve their cyber resilience (Lawyer, 2014).

Other industry frameworks that can be considered when constructing a cyber-resilience strategy include the ISO/IEC Security Control Standards, CIS Critical Security Controls, COBIT, and Cybersecurity Assessment Framework (CAF), to name a few.

Financial services are a target of cyber-criminals looking for financial gain and therefore increasingly need to focus on improving their cyber resilience to minimise the likelihood and impact of attacks (Imeson, 2020).

1.3 Research problem

An adequate response and recovery to a ransomware attack is a concern for South African financial service organisations (Ngila, 2022). An improved cyber resilience posture is a well-understood strategy to mitigate cyber-attacks. There is however, a dearth of information on the extent and effectiveness of cyber resilience strategies for mitigating cyber-attacks being adopted within the South African financial sector.

According to Dupont (2019), though the concept of cyber resilience has become popular in discussions on cybersecurity, it is often seen as difficult to define and measure. However, with organisations coming to terms with the realisation that no organisation is immune to cyber-attacks, cyber resilience strategies offer attractive approaches to effectively mitigate cyber-attacks (Dupont, 2019).

Therefore, it is opportune for a study to investigate the effectiveness of cyber resilience strategies to mitigate ransomware cyber-attacks that can be adopted by South African financial services as part of their cybersecurity strategy.

1.4 Research objectives

The objective of this study is to investigate the cyber-resilient strategies that banks in South Africa are adopting to mitigate and adequately respond to ransomware cyber-attacks. To achieve its objectives, the study will:

- Assess the level of concern and prioritisation that organisations have for ransomware cyber-attacks.
- Investigate the key influences that contribute to the cyber-resilient posture of an organisation against ransomware attacks.
- Assess the role and influence of senior management in influencing the resilient posture against ransomware cyber-attacks.

- Investigate how organisations can evaluate the maturity and effectiveness of cyber resilience as a mitigating strategy.

To support the research objective, below is the main research question and its sub-questions:

Main research question – How effective is a cyber-resilience strategy in mitigating against ransomware related cyber-attacks within South African banks?

Sub-question one - Does financial institutions' cybersecurity strategy prioritize the threat of ransomware?

Sub-question two - What are the factors that influence the cyber resiliency posture of a South African financial institution?

Sub-question three - Can management's involvement in establishing a cybersecurity strategy accelerate the organisations' cyber resilience maturity?

Sub-question four - How can financial institutions assess how well their cyber resilience works as a mitigation strategy?

Using these questions as guidance, the study will investigate strategies that would be effective in reaching a desirable cyber resilient maturity level to mitigate ransomware related cyber-attacks for financial institutions.

1.5 Rationale

Organisations are noted to be accelerating digital transformation through the adoption of technology to enable their strategic objectives (Accenture, 2019). Pancholi et al. (2019) highlights that regardless of an organisation's digital footprint, where an organisation has a reliance on technology, there is an inherent risk of cybercrime. This brings about a pertinent question and point of interest that organisations need to consider in terms of how they would need to go about securing themselves from these cybercrimes.

This study is positioned to contribute to research (and organisations) on areas of focus to curate effective cyber resilience strategies as part of their digital transformation journey.

1.6 Delimitations of the study

The concerns around cyber-attacks span across many different industries, including but not limited to healthcare, telecoms, energy and utilities, construction, financial institutions, etc. (SecurIT, 2021), making it a large scope to consider for a single research study. For the purposes of this study, amongst the various industries, the focus will be placed on financial services, highlighted as one of the industries that is already being pulled towards the digital centre.

To further narrow the scope of this study, the focus will be placed on banking, which, according to Asmundson (2011), primarily offers services such as administering payments, accepting deposits, helping companies buy and sell securities, foreign exchange, and derivatives, and managing assets, amongst many others, as the core function evolves over the years. In South Africa, there are four (4) banks that are commonly cited as the major banks, namely Absa Group Limited, FirstRand Bank, Nedbank, and Standard Bank.

Within the banking sector, there are also areas of focus such as physical security that can be considered when developing a cyber-resilient strategy (Wyss et al., 2007). For this study, physical security will be excluded.

1.7 Assumptions

The assumptions made in this study are that all the main South African banks are on a digital transformation journey and, as a result, would be equally concerned about following an effective cyber-resilient strategy against cyber-crimes. Therefore, all the employees invited to participate in the study from the afore-mentioned banks will be willing to participate as respondents.

Participants will be well versed in the topic of cybersecurity concepts and understand the cyber threat landscape.

The study will be able to collect adequate data for analysis and use within the study, as cyber-resilience is topical and imperative for all the banks to have in place.

1.8 Definition of terms

Cyber Resilience – The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources (Ross et el., 2020).

Cybersecurity – The process of protecting information by preventing, detecting, and responding to attacks (NIST, 2018)

Cyber Threat – Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organisations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service (CSRC, 2015).

Digital Transformation - A unique transformation that organisations undergo, as it depends on understanding the role of data and available technologies, which bring drastic changes to an organization's structure and capabilities (Baslyman, 2022).

Distributed Denial-of-service (DDOS) – A denial of service technique that uses numerous hosts to perform the attack (CSRC, 2015).

Risk - A measure of the extent to which an organization is threatened by a potential circumstance or event, and typically a function of the following: a. the adverse impacts that would arise if the circumstance or event occurs; and b. the likelihood of occurrence. Likelihood is influenced by the ease of exploit and the frequency with which an assessment object is being attacked at present (CSRC, 2015).

Threat Actor – The instigators of risks with the capability to do harm (CSRC, 2015).

Vulnerability - Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source (CSRC, 2015).

1.9 Chapter Outline

The outline of this study is structured with six (6) chapters.

Chapter 1: Introduction

This chapter introduces the research study, outlining the purpose and background of the study, positioning the research problem, and the research objectives coupled with the research questions. This is followed by a view of the delimitations of the study, the definition of the key terms and assumptions made in the study, and finally the chapter outline.

Chapter 2: Literature Review

Following this, chapter 2 outlines the literature review aligned to the proposed research topic, objectives, and questions covered in chapter 1. This is achieved by reviewing specific topics related to the research questions. The section further presents consideration of a theoretical framework and proposes an analytical framework.

Chapter 3: Research Methodology

Chapter 3 outlines the research methodology, covering the research approach and research design, data collection methods, and the procedures for data collection and analysis strategies. The section also covers limitations and challenges anticipated in the study, as well as ethical considerations.

Chapter 4: Research Findings

Chapter 4 outlines findings from the research conducted on South African banks' cyber resilience strategies against ransomware attacks. The section summarises responses from the interviews conducted with various participants working in SA banks and is presented in a narrative format, where verbatim extracts from the interviews are indicated using quotation marks.

Chapter 5: Findings Discussion

Chapter 5 focuses on the discussion of the findings extracted from the semi-structured interviews, linking key points to answering the research question and further supporting a better understanding of the overall research study.

Chapter 6: Conclusions and Recommendations

This chapter provides an overall summary and conclusion of the study in line with the research questions and propositions. Additionally, the researcher provides recommendations as well as suggestions for further research.

2 Literature Review

2.1 Introduction

South African financial institutions are embracing digital transformation, where many organisations are forced to ‘adapt or die’ to continue to be leaders in their respective trades. This drive to adapt has required South African institutions to also relook at their business strategies and operations and leverage technologies to remain relevant in a competitive market (Kekwaletswe & Modiba, 2020).

Inherent to digital transformation in organisations is an increase in cyber threats, which can have a significant impact on their daily operations, especially if the organisations’ cyber resilience is not effective. In a bid to prevent and mitigate cyber threats, the concept of cyber resilience as a strategy has been explored as a potential effective strategy. This chapter aims to review the literature in line with the proposed research topic, research problem, objective, and research questions. The review examines literature that relates to cyber threats, ransomware, cyber resilience, and the role of senior management in the context of building an effective cyber resilience strategy for an organisation.

This section closes out with the analytical framework and conclusion.

2.2 Cyber Threats

2.2.1 Cyber Threat Landscape

The cyber threat landscape is constantly evolving as cyber attackers develop new techniques for attack paths, use new tools, and establish new targets to exploit vulnerabilities (Deloitte, 2014). Cyber threats can have impacts ranging from compromising data confidentiality and integrity as well as availability to disrupting critical infrastructure, which many organisations depend on for business continuity. Materialised cyber-attacks can cause great financial and non-financial impact, including reputational damage and customer loss, and even possibly undermine national security.

Over the past couple of years, the growth of cyber incidents has been noted, impacting even some of the well-known and otherwise well-established organisations such as Solar Winds (Security, 2021), Microsoft, and a Michigan-based bank (Heiligenstein, 2022), amongst many other examples. South Africa has not been immune to cyber incidents, citing examples such as credit bureau Experian, which suffered a data breach; Transnet suffering a ransomware attack; the Justice Department; and the South African National Space Agency also falling victim to cyber-attacks (Moyo, 2022). In 2019, the South African Banking and Risk Information Centre (SABRIC) also confirmed a ransom-driven distributed denial-of-service (DDOS) attack that targeted various South African banks (Fin24, 2019). Furthermore, South African banks have been caught up in third-party exposure where a debt collector (Debt-IN) associated with several SA banks was compromised by a ransomware attack, exposing as much as 1.4 million personal records of South Africans (Moyo, 2021).

It is, however, key to note that globally, cyber-attacks are well reported and documented, where one can only really find reported and well documented cyber incidents up until the end of 2016 (Pieterse, 2021), whereas in the South African context, the maturity of reporting and documenting cyber-attacks is still developing. The assumption is that South African organisations may fear this as an indication of security weakness for their respective organisations.

As noted in the reported incidents, cyber threats come in different forms. Below is a view of four categories of attacks as presented by the Ponemon Institute (2014):

Botnets:

Botnet attacks are cited as being financially motivated. These attacks use multiple networks of infected hosts to run bots on devices, thereafter using all the infected devices to attack an organisation's critical infrastructure, such as their servers, websites, devices, etc. (Ponemon Institute, 2014).

Below is a visual illustration of how a Botnet attack would work:

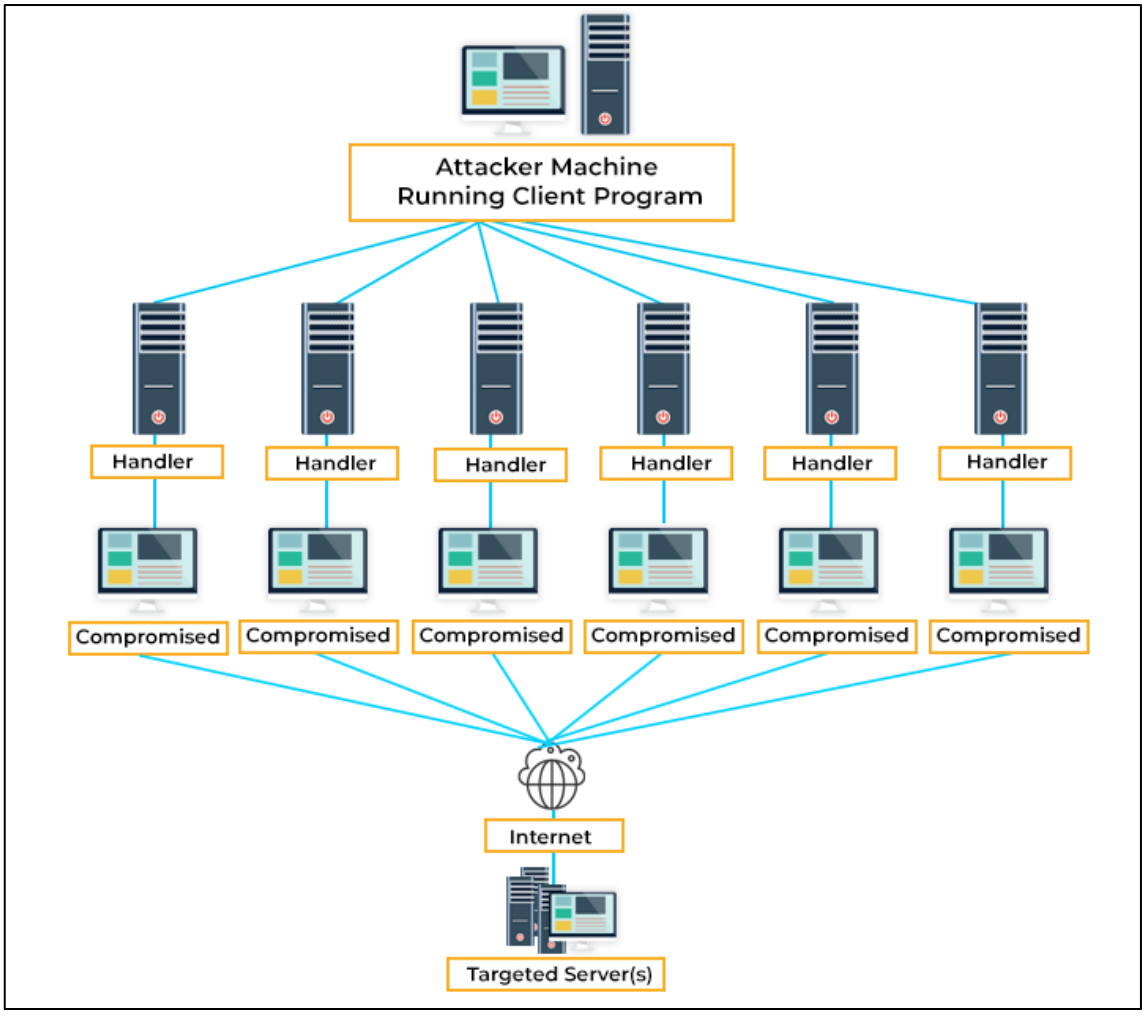


Figure 2 How a Botnet Attack Works (Source: BasuMallick (2022))

Distributed denial-of-service (DDoS) attacks:

A DDoS attack is defined as ‘a denial-of-service technique that uses numerous hosts to perform the attack’ (CSRC, 2015). This type of attack has become popular with threat actors who wish to make a statement, and it is noted that organised criminals use it to blackmail companies, also distracting the incident response teams of organisations while they launch further attacks on the organisation (Ponemon Institute, 2014). One can also note that a botnet is often used in a DDoS attack (Petters, 2020).

Insider Threats:

An insider threat is often caused by an authorised person or entity who can be authenticated and authorised to get past the organisation's security controls (i.e., an employee with privileged access). An attack by an insider often cannot be detected by the organisation's security system, but human behaviour monitoring of employees could help identify if there is a rogue employee who may be motivated to launch an insider attack (Ponemon Institute, 2014).

Advanced Persistent Threats (APTs)

This type of threat is where an intruder successfully gains access to the target's network but remains undetected for a lengthy period while they use the time to collect information on the organisation that they can use at a later stage (Ponemon Institute, 2014). This type of threat is particularly a big challenge to security teams, and they will need the cybersecurity teams to continuously scan the network for any suspicious activity and investigate deception tools where necessary to try to catch the intruder.

Ransomware

Ransomware is commonly understood as a sort of malware that locks down a file on a victim's computer or device and thereafter demands a ransom from the victim. The ransom is usually paid using a payment method that cannot be traced back to the threat actor, such as bitcoin or similar, for the victim to recover access to the compromised system (Kiru & Jantan, 2019).

Below is a visual illustration of how a Ransomware attack would be deployed:

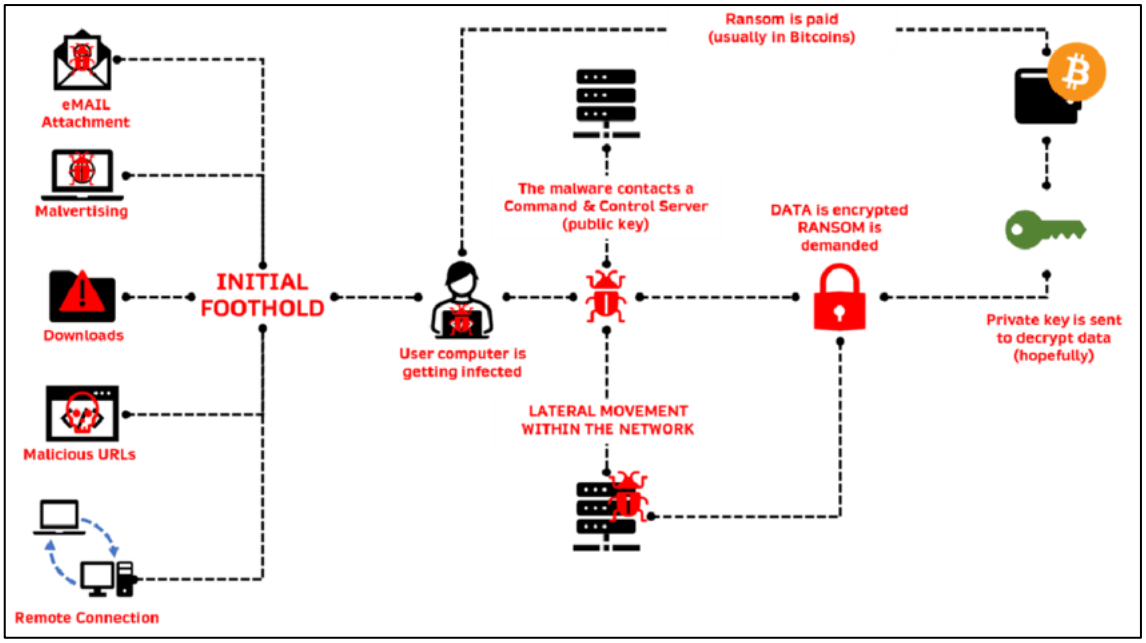


Figure 3 The flow of ransomware works (Source: Leventopoulos (2022))

2.2.2 Cyber-attacks on financial institutions

The growth of cyber-attacks has accelerated cyber risks to financial institutions. Data indicates that attacks are no longer deployed for financial gains but are focused on destroying data, files, or interrupting services or networks (Gulyás & Kiss, 2023). Considering that financial institutions host enormous amounts of data where customers rely on them to keep the data confidential as well as the integrity; additionally, the availability of service is of paramount importance to service customers, this makes financial institutions attractive targets to attackers (Doerr et al., 2022).

According to Gulyás et al. (2023), the underlying question that financial institutions are faced with is no longer whether they will be “attacked or not”, but more of “when” they will be attacked.

A comparison by Petrosyan (2022) of the number of cyber-attacks in financial institutions recorded between 2013 and 2021 indicates a significant rise in cyber incidents in the year 2021. When interrogating the trend, an increase over the years is evident as illustrated in figure 4.

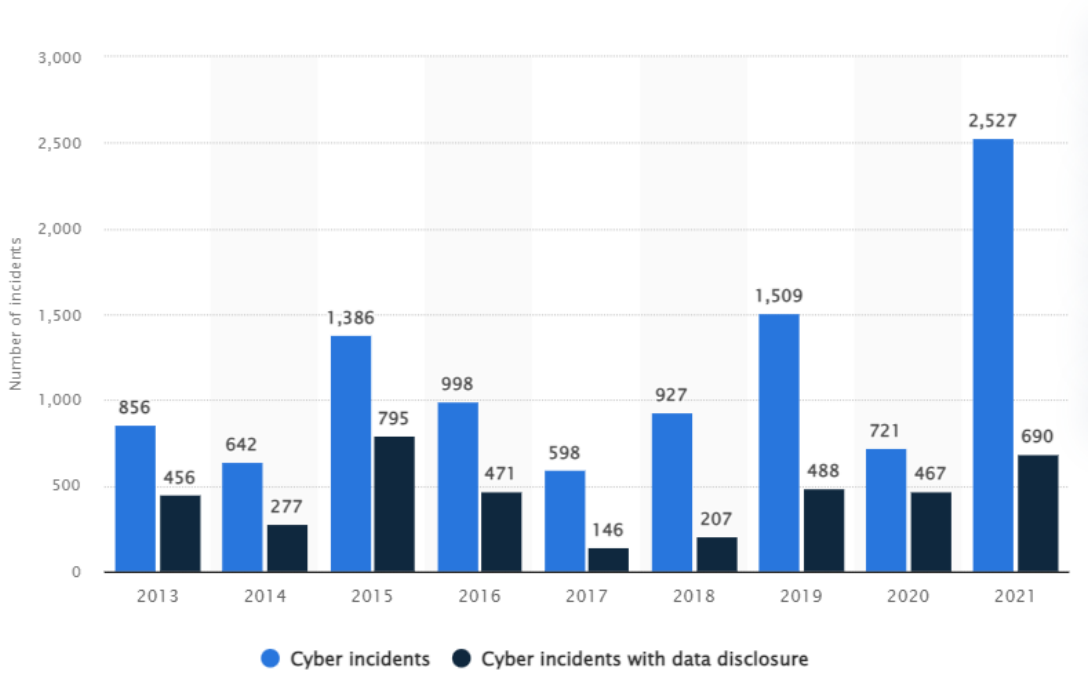


Figure 4 Number of cyber incidents in the financial industry worldwide from 2013 to 2021 (Source: Petrosyan (2022)

The impact of COVID-19 has seemingly also caused a surge in cyber-attacks on financial institutions. Because of COVID-19, organisations, including financial institutions, were forced to conduct their business remotely. This consequently increased the vulnerability of insecure network connections by employees working from home, with indications of up to 47% of individuals proving to likely fall for phishing scams, as well as more than 500 000 people impacted by breaches where their personal data from video conferencing was subsequently stolen and sold on the dark web (Nabe, 2023).

According to Skelton (2017), apart from the impact of cyber-attacks compromising the CIA of a financial institution, the nature of a bank's business increases the risk of a domino-effect impact across all banks in the case of just one of them succumbing to a cyber-attack.

Below are some examples of cyber-attacks that involved financial institutions:

Incident	Impact	Location	Year
Beanstalk Farms cryptocurrency theft	The decentralised finance platform Beanstalk Farms lost $180 million in a cryptocurrency heist.	United States	2022
Fakecalls banking trojan	Banking Trojan Fakecalls, which can ‘talk’ to victims and pretend to be an employee of the bank to gain access to the victims’ contacts, microphone, camera, location and call handling, and attackers attempt to gain payment data or confidential information from the victim.	South Korea	2022
Ronin cryptocurrency theft	Blockchain project Ronin lost $615 million in ether and USD Coin tokens in the second largest cryptocurrency heist to date.	Canada	2022
TransUnion SA data breach	Cyber-attack saw around three million customer's data stolen by a criminal third party.	South Africa	2022

Aon ransomware attack	Aon was hit by a ransomware attack, causing limited disruption to a number of their services.	United States	2022
OCBC phishing scam	790 banking customers of Singaporean bank OCBC were targeted in a phishing scam resulting in a loss of at least $13.7 million.	Singapore	2021
Bitmart security breach	Bitmart, a crypto trading platform, experienced a major security breach, resulting in hackers withdrawing almost $200 million in assets.	Multiple Locations	2021
Taiwanaise Financial institutions cyber espionnage	Attackers ran malicious code on local systems and installed a RAT that allowed them to maintain persistent remote access to the infected system.	Taiwan	2021
Banking trojan targets Indian Android-based financial customers	Android phone banking customers in India were being targeted the Drinik banking trojan malware. The malware stole users'	India	2021

	personal data and funds using phishing techniques.		
German banks hit by DDoS attack on IT provider	A German company that operates technology on the nation's cooperative banks, was hit by a DDoS attack, disrupting more than 800 financial institutions in the country.	Germany	2021

Table 1 Cyber incidents involving financial institutions (Source: (Carnegie, 2023)

The table above provides a view of multiple incidents targeted at financial institutions in just two years – many more of similar examples exist across the globe, highlighting a great concern for financial institutions.

2.3 Ransomware

2.3.1 Origins of Ransomware?

Ransomware, which is well known as malicious malware, has been wreaking havoc in the online world for many years. By encrypting files, it is known to prevent users from accessing their systems (O'Kane et al., 2018). A ransom is requested for victims to regain access to their files.

According to Kansagra et al. (2015), the earliest recorded ransomware attack was in 1989, which was a Trojan called “PC Cyborg” or “AIDS Trojan”. A Trojan, which is understood as malware that disguises itself as a standard programme to hide and mislead its true intent (Crowdstrike, 2017), displayed a message that the user’s licence had expired, and they would need to make a payment to unlock it. According to O'Kane et al. (2018), the creator of the ‘AIDS Trojan’ was a man called Joseph Popp, who is referred to as the founder of ransomware. Later in 2005, another ransomware variant (TROJ_CRYZIP.A) was reported in Russia,

where files were zipped with a password and a ransom note was left for users to pay to access the files (Kansagra et al., 2015). In later years, the evolution of ransomware saw threat actors begin to use encryption of data and request ransom in exchange for the decryption keys.

Over the years, ransomware as an attack path has grown by up to 600% (O'Kane et al., 2018). An evolution timeline for ransomware can be noted in the figure below:

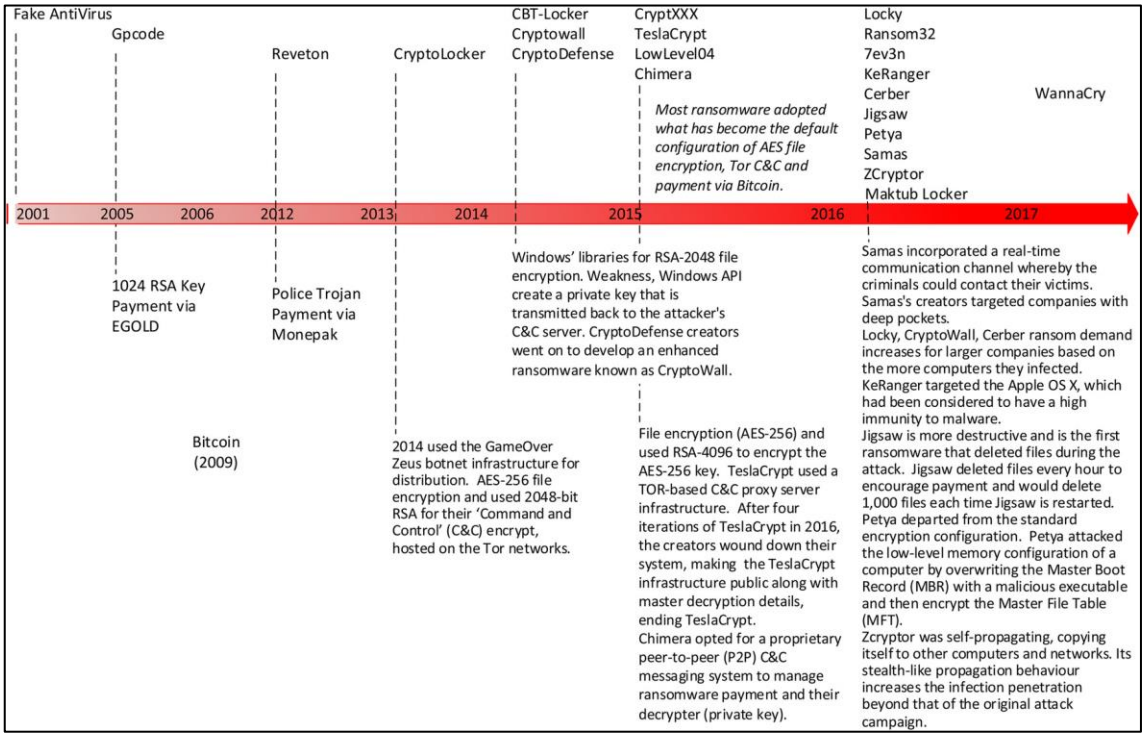


Figure 5 Evolution of Ransomware (Source: O'Kane et al, 2018)

As the attack path evolved, the payment of the ransom also saw an evolution. According to O'Kane et al. (2018), payment methods evolved from threat actors requesting gift vouchers, using payment systems like PayPal, and using prepaid online payment systems such as Paysafecard and Moneypak, which are methods not linked to an individual's bank account, making them difficult to trace. However, the one payment method that has become popular is payment using cryptocurrency, specifically bitcoin, because of the anonymity this method provides, making it close to impossible to trace the threat actor.

2.3.2 Categories of ransomware?

According to Bearman et al. (2021), ransomware can be characterised into three main forms, namely locker, crypto, and scareware, as shown in the figure below:

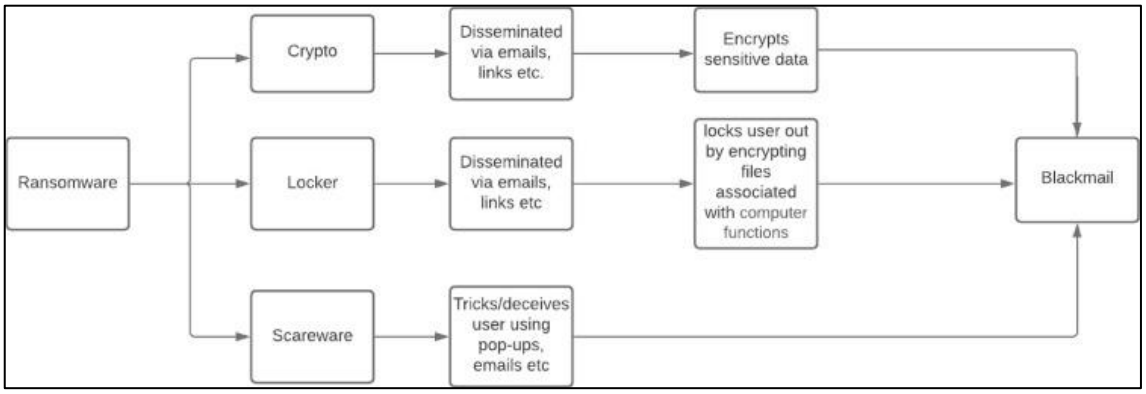


Figure 6 Categories of ransomware (Andronio et al., 2015)

2.3.3 Global trends of ransomware

A preliminary literature review suggests that there is a heightened focus on ransomware at the board level, and organisations are increasing their capability in cyber resiliency in preparation for when an attack does happen (Tuttle, 2021).

Tuttle (2021) further notes that regulators, customers, and shareholders increasingly hold corporate leaders personally accountable for cybersecurity failures, which brings an added level of pressure to senior management and boards of financial services as they are highly regulated, and the nature of their business has a direct impact on customers and shareholders.

Some of the attack methods or patterns include the use of social engineering tactics or phishing campaigns to gain administrative privileges, where the threat actor can make lateral movements within the network and exploit vulnerabilities. If an attacker is successful in gaining administrative privileges, they are also able to start gathering data, which can then later be used to bargain for ransom. According to Aurangzeb et al. (2017), ransomware attacks all follow similar characteristics, which include device locking, data encryption, data deletion, data stealing, and sending threatening messages. The detection of the evolving

techniques used is noted to be maturing, with ongoing investigations to improve the effectiveness of detecting new patterns (Kapoor et al., 2021).

When considering trends, one key trend that has also been recorded is that attackers target organisations' backups first and use this as bargaining leverage for ransom to be paid. This is due to the organisation's previous reliance on their backups for business continuity, which they could restore. The risk, however, remained that threat actors could still sell or leak personal information that was stolen, which would still compromise the confidentiality of data that organisations keep.

According to a report by MARSH (2023), a global leader in insurance broking and risk advisory, ransomware attacks are 'intensifying in frequency, severity, and sophistication. Below reflects the statistics collected by MARSH.

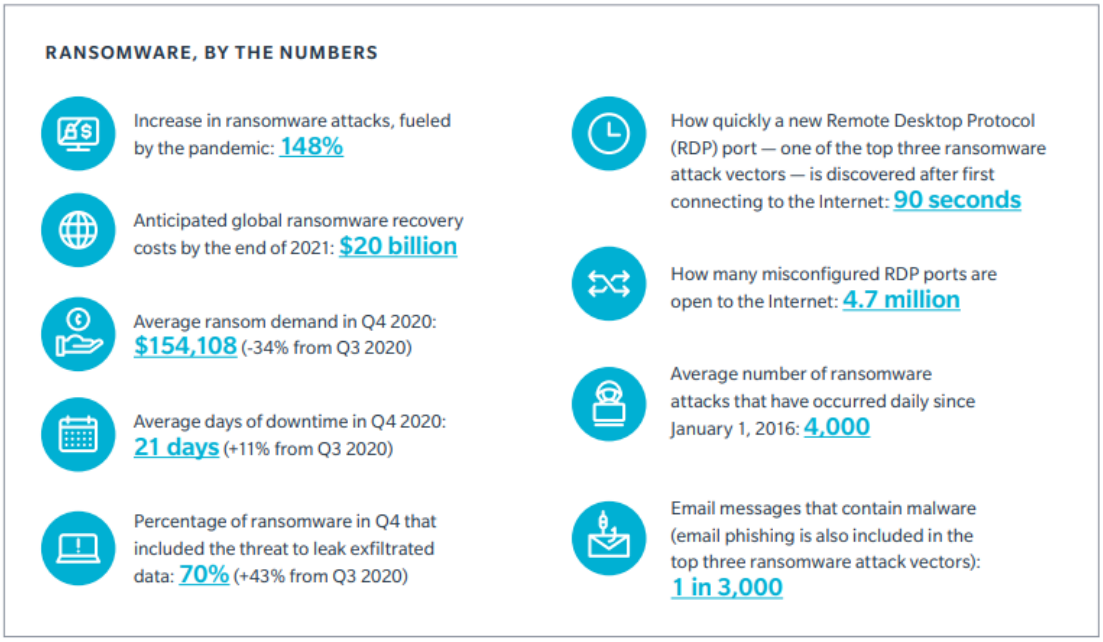


Figure 7 Ransomware by the numbers (Source: (MARSH, 2023)

2.3.4 Impact of ransomware on South African Banking sector

Although ransomware is not a new phenomenon, it has recently become more common and sophisticated because of the accessibility of encryption technologies, anonymous payment methods, and exploit kits, with COVID-19 exacerbating ransomware attacks on various institutions within healthcare,

financial services, and government (Bearman et al., 2021). Financial institutions, in particular banks, may suffer severe harm because of ransomware attacks, which includes financial losses, operational and availability impacts, reputational damages, and regulatory impacts resulting in fines. The financial losses can be attributed to having to pay the ransom, as well as indirect financial losses such as customer attrition, loss of trust, recovery efforts, loss of opportunities, and regulatory fines. The impact further goes into legal obligations on duty to take care of customer personal data, which may be compromised because of a ransomware attack (Akinbowale et al., 2023; SABRIC, 2019; Ogunjuyigbe, 2020).

Stats and Trends

According to SABRIC (2023), 13 438 incidents across banking apps, online banking, and mobile banking cost the industry more than R250 000 000 in gross losses. It is, however, not clear how many of these incidents are ransomware. The researcher also notes that there is a dearth of information in the literature relating to ransomware attacks in the South African banking sector.

The following ransomware incidents occurred in South African financial institutions, some of which were banks, according to a timeline by Carnegie (2023).

Incident	**Impact**	**Location**	**Year**
Dexter Malware hits South Africa's Banks	Hackers infected electronic point-of-sale terminals with a malware called Dexter, allowing them to breach most major South African banks and make off with millions of rand	South Africa	2013

South African Insurer Ransom Attack	South African insurer Liberty Holdings was targeted by hackers who claimed to have seized data from the firm. The hackers threatened to publicly disclose the data unless compensated.	South Africa	2018
SABRIC DDoS Attacks	The South African Banking Risk Information Centre (SABRIC) reported a series of distributed denial-of-service attacks which targeted several public facing services across multiple banks in the country. The attacks started with a ransom note delivered via email to several publicly available addresses.	South Africa	2019
South African debt collector ransomware attack	Debt-IN Consultants, a South African debt collector, was hit by a major ransomware attack, resulting in a significant data breach of consumer and employee personal information. The data of more than 1.4 million South	South Africa	2021

	Africans was illegally accessed from the company's servers, with confidential consumer data and voice recordings of calls between Debt-IN debt recovery agents and financial services customers posted on the dark web		

Table 2 Cyber incidents involving financial institutions (Source: (Carnegie, 2023)

2.4 Cyber Resilience

2.4.1 Defining Cyber Resilience

Dupont (2019) defines cyber-resilience as "the capacity to withstand, recover from, and adapt to the external shocks caused by cyber risks." Dupont (2019) further cites that cyber-attacks have become inevitable, and even mature financial institutions would not be able to eliminate threats despite the amount of investment they make in cybersecurity technologies. In the cybersecurity industry, one often hears the phrase "it's not if an attack will happen, but rather when it will happen" (Pearlson et al., 2021). The key question subsequently becomes, 'How prepared is the organisation to be in a position to detect, respond, and recover accordingly?' These are key activities within a cyber-resilient strategy for mitigating attacks. Pearlson et al. (2021) cite that 47% of organisations have not yet assessed their incident response teams, which potentially means that when an attack does take place, the impact could have dire effects (Ponemon Institute, 2014).

2.4.2 Understanding Cyber Resilience as a strategy

According to Johnson et al, (2011), strategy is defined as:

> "…the direction and scope of an organisation over the long term. It achieves advantage for the organisation through its configuration of resources within a changing environment to meet the needs of markets, customers, or clients and to fulfil stakeholder expectations."

In line with Johnson et al.'s (2011) definition of strategy, ensuring that an effective cybersecurity strategy is in place not only ensures that the operations of organisations are safeguarded but also ensures that customers or clients are safeguarded against potential cyber threats. In the context of cybersecurity, taking into consideration the rapid growth of cyber-attacks, with ransomware being one of the most noticeable attack paths, any organisation operating digitally will need to ensure that they have an effective strategy in place specific to building the cyber resilience of that organisation.

However, Conklin et al. (2017) argue that there is not any industry that has managed to develop an effective standard strategy to protect itself against the growing cyber-attacks. While many adopt and focus on protecting the logical points of access, this strategy still leaves organisations' critical assets vulnerable to being compromised by a cyber-attack. According to Conklin et al. (2017), adopting cyber-resilience as a strategy means that an organisation would focus on protecting their most critical assets to reduce the business impact in the event of an attack. Additionally, cyber-resilience ensures that the correct resources are in place to detect any malicious activity, and where, in an unfortunate event, the attack is successful, the organisation needs to be able to respond and recover as quickly as possible to reduce service impact. Therefore, having a cyber-resilient organisation would require well-defined processes to effectively respond to attacks and any successful penetration to prevent the attacker from reaching and compromising the organisation's critical assets. To support the adoption of cyber-resilience as a strategy, according to Dupont (2019), for organisations to have an advantageous position against cyber threats, they would need to look at adopting cyber-resilience as a complementary alternative to an existing cybersecurity paradigm.

Conklin et al. (2017) share seven generic principles, which are described as the “Cyber Resilience Process”, discussed below. The principles outlined are closely aligned and comparable to the various steps outlined in the NIST framework.

Classify: The principle of classification puts emphasis on the fact that you cannot protect assets you do not know exist. To classify assets, organisations need to identify, label, and sort all assets, which can be used to determine things like which assets are considered critical to business operations, therefore taking precedents in protection, backing up first, and ensuring quick recovery. This principle is comparable to the “Identify/Classification” step of the NIST Framework (NIST, 2014).

Risk: To ensure effective resiliency, organisations need an appropriate and well-communicated risk appetite. A risk assessment considering various threat scenarios is key to determining how much risk the organisation is potentially exposed to. The risk-based approach also assesses internal controls and the application thereof. This principle is comparable to the NIST step “Assessing Security and Privacy Controls in Information Systems and Organisations” (NIST 800-53A, 2022).

Rank: Organisations need to have clear visibility of their critical and non-critical assets to deploy the correct resources for the best possible chance of having a minimal impact in the event of an attack. To be able to get to such a view, the “rank” principle looks at ranking an organisation's assets according to their criticality. This principle is comparable to the NIST step of "select," which serves the purpose of ensuring that the correct controls are tailored and selected to protect the organisation’s critical assets in line with the risk appetite (NIST, 2023).

Design/Deploy: For resilience to be effective, resilience controls need to be embedded in the architecture and design thereof. This principle is comparable to the NIST step of "implement," which is focused on how specific security and privacy controls are implemented within the organisation to ensure a level of resilience (NIST, 2023).

Test: Once all controls have been applied, this principle serves to assure that resilience can be achieved through testing. During this step, methods such as penetration testing can be used to test the resilience of the implemented controls. The “test” principle is comparable to the “assess” step of the NIST framework, which serves the purpose of assessing whether the implemented controls are operating as intended, effective, and producing the desired outcome of ensuring resilience (NIST, 2023).

Recover: In the case of a realised attack, an organisation needs to be able to quickly recover. To do this effectively, a recovery plan needs to be established, well documented, and even tested to ensure a seamless and full recovery. This principle is comparable to the “recovery” function of the NIST framework (NIST, 2018).

Evolve: To keep up with the ever-changing threat landscape, organisations need to be agile and dynamically adjust various security controls, processes and even architecture to remain cyber resilient. Adjustments can be derived from lessons learned internally and externally, outcomes from the test phase or even from continuous monitoring and observations of key changes from the threat landscape. This principle is comparable to the “Monitor” step of the NIST framework (NIST, 2023).

2.5 Frameworks and best practices that inform cyber resilience

Cybersecurity, as defined to be ‘the process of protecting data and systems from theft and being damaged'—in order for an organisation to successfully achieve this, there are a set of standards, processes, and frameworks that can help guide them in implementing cybersecurity across the different levels of their business (Taherdoost, 2022).

According to Taherdoost (2022), standards are ‘documents or rules made based on a general agreement and validated by a legal entity that help to achieve optimal results as a guideline, model, or sample in a particular context’, where standards provide organisations with the necessary guidelines for successful

compliance and governance that can assist organisations in obtaining desired results. Standards are also said to ensure the safety, reliability, and consistency of services, products, and systems for organisations. Furthermore, frameworks are introduced in industry to provide a guideline to organisations on specific domains, which can be adopted by each organisation. It is important to note that a framework does not prescribe for an organisation to adopt specific options but rather acts as a guidance note for organisations (Taherdoost, 2022).

The main objective of standards and frameworks within the cybersecurity field is to assist organisations in preventing and mitigating cyber-attacks, as well as reduce the risks of cyber threats.

In the field of cybersecurity, there are several standards and frameworks available for organisations to adopt. Below is a description of some popular standards and frameworks taken from available literature:

2.5.1 ISO 27000 Series

ISO 27000 is an internationally recognised standard that focuses on information security. This standard is designed to help organisations manage their information security by focusing on the people, processes, and technology aspects of an organisation. ISO 27000 is commonly used in conjunction with ISO/IEC 27001, where the latter is used to ensure the effective implementation of information security in an organisation.

2.5.2 NIST Cybersecurity Framework

The framework is a voluntary framework that helps organisations understand and improve their management of cybersecurity risks (NIST, 2018).

The NIST framework consists of five core functions, with the categories and sub-categories derived from various industry best practices, standards, and guidelines. The five core functions are designed to offer a high-level and strategic view of an organisation's lifecycle in the management of cybersecurity risk (NIST, 2018).

The NIST framework is one that many organisations align with as an industry best practice for their cybersecurity and, in turn, for building their cyber resilience. The NIST framework is recommended to be used in conjunction with any implemented frameworks in organisations to complement rather than replace them (Almuhammadi & Alsaleh, 2017).

The NIST framework consists of five core functions, with the categories and sub-categories derived from various industry best practices, standards, and guidelines. The five core functions aim to offer a high-level and strategic view of an organisation's lifecycle in the management of cybersecurity risk (NIST, 2018).

The five core functions are described below. Important to note is that these functions are not prescribed to organisations but rather to offer a static end state for the organisation's cybersecurity programme.

Identify:

For an organisation to adequately put cyber-attack mitigation strategies in place, they would need to ensure that they have a full inventory of key elements within their business, such as critical information, company assets, and existing capabilities. The ‘identify’ function’s objective is to help guide organisations to identify and adequately manage their cybersecurity risk to systems, people, assets, people, data, and capabilities. Categories within this function include asset management, business environment, governance, risk assessment, and risk management strategy (NIST, 2018).

Protect:

An organisation has a mandate to protect their critical infrastructure as well as to ensure that there is minimal impact in the event of a cyber-attack. The ‘protect’ function provides guidance to organisations on how to develop and implement appropriate safeguards for critical infrastructure. The categories of this function include identity management and access control; awareness and training; data security; information protection processes and procedures; maintenance; and protective technology (NIST, 2018).

Detect:

In a case of a cyber-attack, to potentially minimise the impact thereof, an organisation needs to be able to swiftly detect the activities of cybersecurity events. The ‘detect’ function assists organisations to timely discover cybersecurity events, where they can use various tools and techniques to achieve this. Categories of this function include anomalies and events; security continuous monitoring; and detection processes (NIST, 2018).

Respond:

Once a cybersecurity event has been detected, the cybersecurity team needs to be able to respond accordingly to minimise the impact of the attack. The ‘respond' function offers guidance on how organisations can develop and implement suitable actions and activities once a cybersecurity incident has been detected. Categories within this function include response planning, communications, analysis, mitigation, and improvements (NIST, 2018).

Recover:

In the unfortunate case of a successful cyber-attack or intrusion, an organisation will need to ensure that they are able to recover in a timely manner to avoid a severe and widespread impact on business and customers alike. The 'recover' function thus provides guidance around this in terms of how organisations can develop and implement activities required to maintain resilience plans, including backing up critical systems and restoring any impacted capabilities and services. Categories within this function include recovery planning, improvements, and communications (NIST, 2018).

2.5.3 COBIT

Control Objectives for Information and Related Technologies (COBIT) is a framework that was developed by the Information Systems Audit and Control Association (ISACA). ICASA is an independent organisation made up of governance professionals with the main objective of helping organisations get a balance between their IT and business goals by bridging the gap between

technical issues experienced by organisations and business risks (Taherdoost, 2022).

The COBIT framework offers five (5) principles that are designed to guide the effective management and governance of an organisation. The five principles include:

1. **Meeting Stakeholder Needs**, focused on the importance of getting a buy in from all stakeholders.
2. **Covering the enterprise end-to-end** by integrating governance IT into enterprise governance, ensuring that the focus is not only placed on the IT function but treats information and related technologies as assets.
3. **Applying a single integrated framework** by serving as an overarching governance framework which aligns with all the other relevant standards and frameworks.
4. **Enabling a holistic approach** to ensure that all areas are adequately considered and covered.
5. **Separating Governance from Management**, where governance remains the responsibility of the board of directors under the leadership of a chairperson, and management is the responsibility of the executive management under the leadership of the CEO.

The five principles are designed in such a way that an organisation would be able to create a holistic framework for its governance and management of its IT infrastructure (IT Governance, 2022).

2.6 Evaluation methods of cyber-resilience

As the frequency and sophistication of cyber-attacks rapidly grow, while organisations focus on improving their cyber-resilience, one of the key actions they ought to consider is to test or evaluate the effectiveness of the employed cyber-resilience strategy to ensure that they are adequately prepared in case of an attack (Bodeau et al., 2018). There are several evaluation methods that organisations use to evaluate the effectiveness of their cyber-resilience strategies. The testing is focused on the assessment of the organisations' ability

to prevent, detect, respond, and recover from cyber-attacks (Lee, 2016). While each of the evaluation methods has its own strengths and weaknesses, organisations have the responsibility to consider which assessments will be a good fit for their respective organisations. Below is a description of methods and frameworks identified from the literature that can be used to evaluate the effectiveness of cyber resilience.

2.6.1 Cyber Resilience Review (CRR)

The Cyber Resilience Review is a framework created by the U.S. Department of Homeland Security aimed at providing a comprehensive evaluation and measurement of an organisation's operational resilience capabilities and cybersecurity practices. The CRR is created using guidance from the Cyber Resilience Evaluation Method and the CERT Resilience Management Model (CERT-RMM) (U.S. Department of Homeland Security, 2020). The method of assessment employed by this framework is in the form of an interview-based assessment facilitated in a workshop style where critical questions are posed on topics including critical infrastructure, the organisation's personnel in cybersecurity, operations, physical security, and business continuity. According to the U.S. Department of Homeland Security (2020), the assessment can be replicated as it uses the same questions, scoring mechanisms, and options for improvement. When conducting the assessment, the framework focuses on ten domains where it seeks to assess and understand the capacity and capabilities that an organisation has in relation to planning, managing, measuring, and defining the cybersecurity practices and behaviours conducted (U.S. Department of Homeland Security, 2020). Each of the domains outlined has a purpose statement to provide an overview and intent of the domain, specific goals and practices that are unique to the domain and are assessed accordingly, and finally a maturity indicator level (MIL), which is also assessed through questions. The ten domains and how they relate to the number of goals, practices, and maturity indicator level are illustrated in the figure below:

CRR Domain	No. of Goals	No. of Goal Practices	No. of MIL* Practices
Asset Management	7	30	13
Controls Management	4	16	13
Configuration and Change Management	3	23	13
Vulnerability Management	4	15	13
Incident Management	5	23	13
Service Continuity Management	4	16	13
Risk Management	5	13	13
External Dependencies Management	5	14	13
Training and Awareness	2	11	13
Situational Awareness	3	8	13

* Maturity Indicator Level

Figure 8 CRR Domain Composition (Source: U.S. Department of Homeland Security (2020))

Once the assessment is completed, a report is produced highlighting all the gaps and cybersecurity improvement areas, along with recommendations and considerations that are based on recognised standards and industry best practices (U.S. Department of Homeland Security, 2020).

2.6.2 Cyber-resilience assessment framework (C-RAF)

The cyber-resilience assessment framework is a framework that was released by the Hong Kong Monetary Authority (the "HKMA") in November 2020. The framework is designed as a risk-based framework where organisations can use it to assess their own cyber risk profiles and benchmark their respective cyber resilience to determine whether it is effective or not against potential attacks (Deloitte, 2023). The C-RAF features a two-part self-assessment and an intelligence-led cyberattack simulation test (iCAST) (Carter & Crumpler, 2019). The self-assessment component is based on and guided by various other frameworks, including the FFIEC Cybersecurity Assessment Tool (CAT), the NIST Framework, and the BIS/IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures, which evaluates security systems against 366 controls derived from these frameworks.

In the framework's three-step approach, an assessment of the organisation's inherent risk is determined by considering key factors, including technologies

used, delivery channels adopted, activities, products, services, infrastructure, operating environment, where an inherent risk rating is applied to each aspect. The 'inherent risk rating' is then further mapped to an expected "maturity level," (see figure below for a visual representation of the mapping).

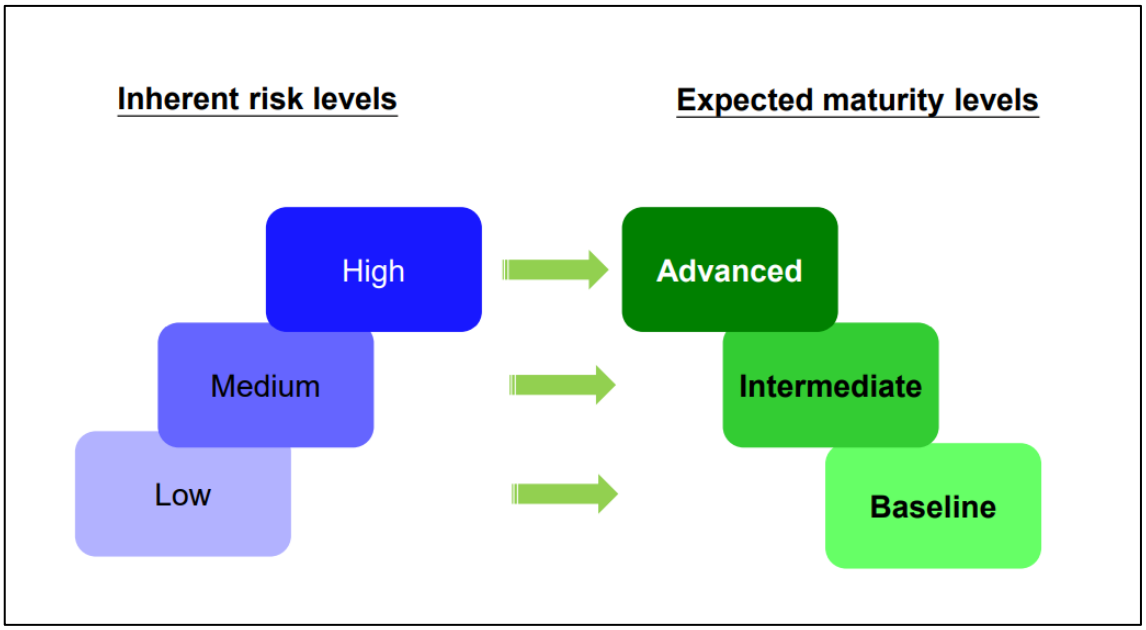


Figure 9 Inherent Risk Rating mapping to Expected Maturity Level (Source: Lee (2016))

The second step of the approach assesses the maturity of the seven domains, with the key objective of determining the level of resilience maturity in each domain and later components. The seven domains of the maturity assessment can be seen in the below figure:

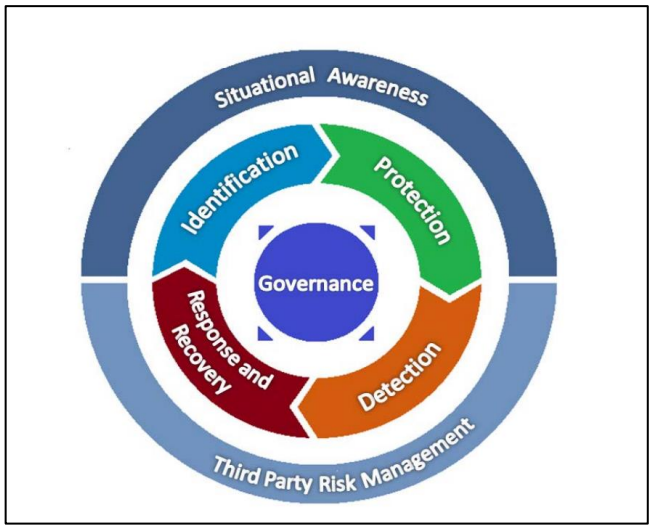


Figure 10 Maturity assessment (in seven domains). (Source: Lee (2016))

Each of these domains is made up of further components, which can be seen in the figure 2.11 below:

	Domain	Component
Governance	Governance	Cyber resilience oversight
		Strategy and policies
		Cyber risk management
		Audit
		Staffing and training
Internal environment	Identification	IT asset identification
		Cyber risk identification and assessment
	Protection	Infrastructure protection controls
		Access control
		Data security
		Secure coding
		Patch management
		Remediation management
	Detection	Vulnerability detection
		Anomalies activity detection
		Cyber incident detection
		Threat monitoring and analysis
	Response and recovery	Response planning
		Incident management
		Escalation and reporting
External environment	Situational awareness	Threat intelligence
		Threat intelligence sharing
	Third party risk management	External connections
		Third party management
		Ongoing monitoring on third party risk

Figure 11 Components of the maturity assessment (Source: Hong Kong Monetary Authority, 2016)

Once the assessments in the two steps have been completed, the outcomes from both the inherent risk assessment and the expected maturity assessment are then compared, where gaps are identified for consideration and a remediation roadmap is put together to address the gaps (Hong Kong Monetary Authority, 2016).

Where an organisation has an inherent risk rating of “medium” or “high,” the Cyber Resilience Assessment Framework requires intelligence-led cyber-attack simulation testing (iCAST) to be conducted. The iCAST requires comprehensive penetration testing based on test scenarios to determine the effectiveness of existing controls and help identify any existing gaps (Carter & Crumpler, 2019). Traditional penetration testing is commonly known to have the limitation of only focusing on technical assessments; however, the assessment conducted as part of the iCAST extends the testing to “people and processes” (Lee, 2016). Further to this, penetration testing under iCAST is augmented by including threat information and additional knowledge verification of the penetration tester(s) to the typical penetration test to create end-to-end testing scenarios, allowing for simulations close to real-life attacks (Hong Kong Monetary Authority, 2016).

2.6.3 Assurance Reviews

Assurance is a method that is used to provide confidence in the implemented security controls, highlighting their effectiveness. While there are many ways to provide assurance in this regard, the National Cyber Security Centre (2023) discusses four common methods:

Method	**Description**

Self-Assessment	In this method, the internal cybersecurity teams assess and report of the effectiveness of the implemented controls. This can be completed by answering pre-determined questions. The evaluation of the effectiveness is however subjected to the individuals performing the assessment.
Internal Assessment	Internal assessments are usually performed by staff members such as Internal Audit teams. Whilst this team may be employed by the organisation, the assessments are conducted independent from the security teams to provide a more objective assessment.
External Assessment	External assessments can take various forms, including table-top exercises, simulating breaches, benchmarking against industry standards and penetration testing. This type of assessment provides an objective evaluation by testing the various points of vulnerability.
Automated Assessment	Automated assessments make use of in-built testing, monitoring, and reporting. This may often work well on technology systems rather than the assessment of processes or people.

Table 3 Common Assurance Methods (Source: National Cyber Security Centre (2023)

2.6.4 Metrics

Metrics are defined as “the result of a process or method for measuring, evaluating, or comparing similar objects” (Bodeau et al., 2018). According to Bodeau et al. (2018), metrics can be used by the organisation to identify and describe how well the implemented controls, efforts, and even performances enable achieving the objectives of cyber-resilience; metrics can also be used as

a tool for learning and decision-making. The National Cyber Security Centre (2023) supports the idea that metrics and indicators are used to inform decisions in an organisation, which will enable effective operation. Metrics can enable an organisation to consistently track the effectiveness of their cybersecurity programmes.

While security and resilience metrics are closely related to risk metrics, there are some nuanced differences (Bodeau et al., 2018). In the table below, the differences in the metrics are outlined and are to be considered when creating metrics specific to cyber resilience:

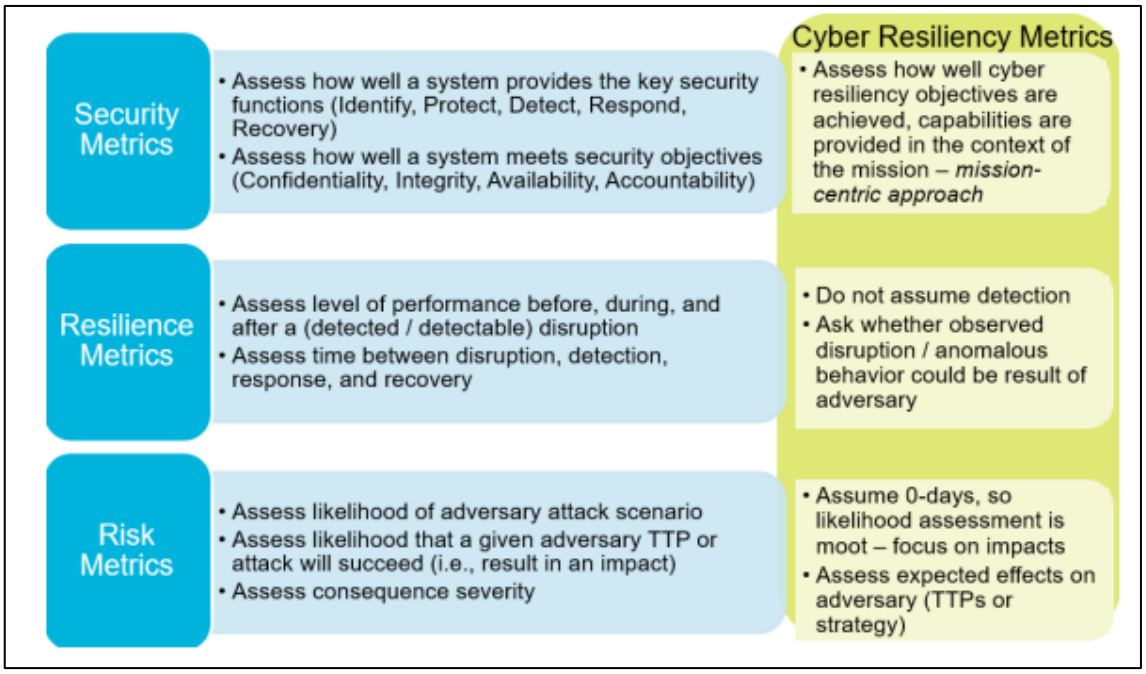


Figure 12 Cyber Resiliency Metrics Can Repurpose Security, Risk, or Resilience Metrics (Source: Bodeau et al., (2018))

Metrics are noted to be best used on a continuous and consistent basis to inform items such as trends, address gaps through remediation efforts, and help inform the adjustment of security programmes.

2.7 Senior Management and Cyber resiliency

2.7.1 Management's awareness of ransomware as a top risk

Literature suggests that there is a heightened focus on ransomware at the board level, and organisations are increasing their capability in cyber resilience in preparation for when an attack does happen (Tuttle, 2021).

Tuttle (2021) further notes that regulators, customers, and shareholders increasingly hold corporate leaders personally accountable for cybersecurity failures, which brings an added level of pressure to senior management of financial services as they are highly regulated, and the nature of their business has a direct impact on customers and shareholders. According to Bajpai & Enbody (2020), senior management has regarded ransomware as a top threat and concern. Brewer (2016) further highlights the amount of money that is lost annually by organisations because of ransomware, which has certainly gotten the attention of senior management to pay closer attention to preventing and mitigating any potential ransomware attacks. Contrasting this view, according to Triplett (2022), many of the senior management still view cyber threats as "a technological catastrophe", which tends to place focus and often pressure solely on the IT department to "sort things out".

Although organisations adopt various approaches in their business model, Asana (2021) suggests that a top-down approach works better for organisations to achieve some of their complex business decisions. Where cyber resilience is concerned, it is imperative to have alignment across all levels of the organisation, with the executive and board members on board with the cyber resilience plans.

*2.7.2 **Role of senior management in ensuring cyber-resilience***

The role of strategic leadership in an organisation is of paramount importance when trying to establish an effective cyber resilience strategy against rapidly rising cyber threats. It is important to note that cybersecurity and cyber resilience are not just the business of the IT department but of the organisation at large, with senior management leading by example.

Lending from the idea of “leading by example,” literature points us in the direction that, when it comes to building cyber-resilience, humans are considered the weakest link. According to Triplett (2022), the human element should remain at the centre of any business operations, and more so in building cyber resilience. This is supported by the notion that humans are more susceptible to making errors such as the use of weak passwords, clicking on malicious phishing links, or even being targeted through social engineering, all of which are potential exploitable points for cyber criminals. Triplett (2022) proposes that one of the key roles that senior management should play in building cyber resilience is to actively promote cyber education and training. The promotion of cyber education and training is further supported by Al-Alwawi et al. and Al-Bassam (2019), who discuss the importance of staff training on matters of cybersecurity, despite the role any individual fulfils in the organisation. Promoting the training and education of cybersecurity across the organisation increases the defences and thus resilience against potential cyber threats, as well as subsequently promoting a cyber-aware culture across all staff.

While literature indicates that to ensure a cyber-resilient organisation, all staff members need to be well trained and actively partake in the safeguarding of the organisation, there still needs to be an overall driver and an accountable person or persons for cybersecurity. When it comes to senior management or the senior leadership team, traditionally there are a number of c-suite titles to consider, including but not limited to CEO, COO, CFO, and CIO. As a result, organisations have actively moved to employ a Chief Information Security Officer (CISO) to take the overall driving seat in influencing a cyber-resilient posture for the organisation with the support of the rest of the c-suite (Reilly et al., 2016). With this role, Triplett (2022) positions that this leader will need to be a person who can effectively communicate with the board and rest of business on issues relating to cybersecurity, but also be able to relate and provide guidance to the IT teams doing the groundwork. This stance is equally supported by Bagheri et al. (2023) who further explain that there needs to be a mutual understanding on issues of cybersecurity across all senior leadership to cascade and align this with the rest of the business.

One other key role played by senior management in building a cyber-resilient organisation is that of effective budgeting and correct allocation of funds. It is well understood that investing in various technologies can be an expensive exercise, and one cannot solely rely on technology to be a silver bullet for building cyber-defences for an organisation. According to Al-Alawi et al. (2019), senior management needs to place cybersecurity as a top priority, and this should reflect in the budget allocations to ensure that the organisation is armed with sufficient resources and security controls to promise adequate cyber-resiliency.

Overall, the literature illustrates that the buy-in and support from senior management in building an effective cyber-resilience strategy for an organisation is of paramount importance.

2.8 Analytical Framework

According to Gale et al. (2012), an analytical framework is defined as “a set of codes organised into categories that have been jointly developed by researchers involved in analysis that can be used to manage and organise the data. The framework creates a new structure for the data (rather than the full original accounts given by participants) that is helpful to summarise or reduce the data in a way that can support answering the research questions.”

Lending from this definition, an analytical framework is the underpinning structure to assist a researcher in guiding and facilitating the sense-making of various theories and models in a research study.

In this section, different theories and models will be discussed under ‘theoretical frameworks and a conceptual framework will be positioned as a guide for this study.

2.8.1 Theoretical Framework

According to Grant & Osanloo (2014), the theoretical framework is an important aspect of the research process that influences various parts of the research, including the selection of a topic, the development of research questions, the design approach, and the analysis plan.

This study will consider the Routine Activity Theory (RAT).



Figure 13 Routine Activity Theory (RAT) (Source: Govender et al., (2021)

Routine Activity Theory, as illustrated in Figure 1, is cited as a model that was initially framed by Lawrence E. Cohen and Marcus Felson in 1979 and is commonly used in the study of criminology and crime science (Miro, 2014). Although RAT is commonly used for studies in criminology and crime science, authors such as Govender et al. (2021) have applied this theory to cybercrime-related studies. Furthermore, through an analysis, Leukfeldt & Yar (2016) position RAT as a suitable theory to test cyber-related crimes, additionally highlighting that, depending on the study, some of the RAT elements may be more applicable than others.

For the purposes of understanding the elements that are evaluated through RAT, Miro (2014) shares that RAT is made up of three (3) essential elements, namely (a) a likely offender, (b) a suitable target, and (c) the absence of a capable guardian. Where there is a convergence of the three elements, the theory concludes that a crime would take place. For this study, the researcher will focus on the element of 'the absence of a capable guardian.'

The likely offender is identified as a person who would have a motive to commit a crime as well as the capability and capacity to conduct a crime (Felson & Cohen, 1980). In the context of this study, a likely offender would be a threat actor who

has the skills, capability, and, at times, the funds to launch a cyberattack by exploiting open vulnerabilities (CSRC, 2015).

A suitable target is identified as “a person or property that may be threatened by an offender” (Miro, 2014). A suitable target is often considered to hold something of value that the likely offender can benefit from. In this instance, a suitable target would be a South African financial institution or bank that is positioned as a potential big pay-out target after being challenged by the emergence of various fintech companies to transition into digital businesses for both their business and customer strategic objectives (Ledesma, 2021). While the adoption of digital services and processes alike offers vast benefits, it also comes with the risk of increased cyber-attacks, and, more recently, a looming ransomware attack where threat actors may hope to get big payouts due to the nature of the data and service offerings that financial institutions have (Ledesma, 2021).

The RAT theory adds a third element, which is ‘the absence of a capable guardian.’ A capable guardian is described as someone or something that can intervene or help mitigate a crime from taking place (Cohen & Felson, 1979).

Miro (2014) explains that a guardian who can prevent a crime is one who, when present or applied, would prevent a crime from happening; however, in a case where a capable guardian is absent, a crime taking place will become more probable. In the case of this study, a capable guardian refers to the cybersecurity posture of a financial institution, where the various security controls and measures are employed by an organisation to safeguard against a probable cyber-crime. Govender et al. (2021) support this proposition by stating that guardianship in the form of security measures is essential in protecting a suitable target from a likely offender (cyber threat actors).

A presupposition of the proposed use of RAT in the study is depicted below:

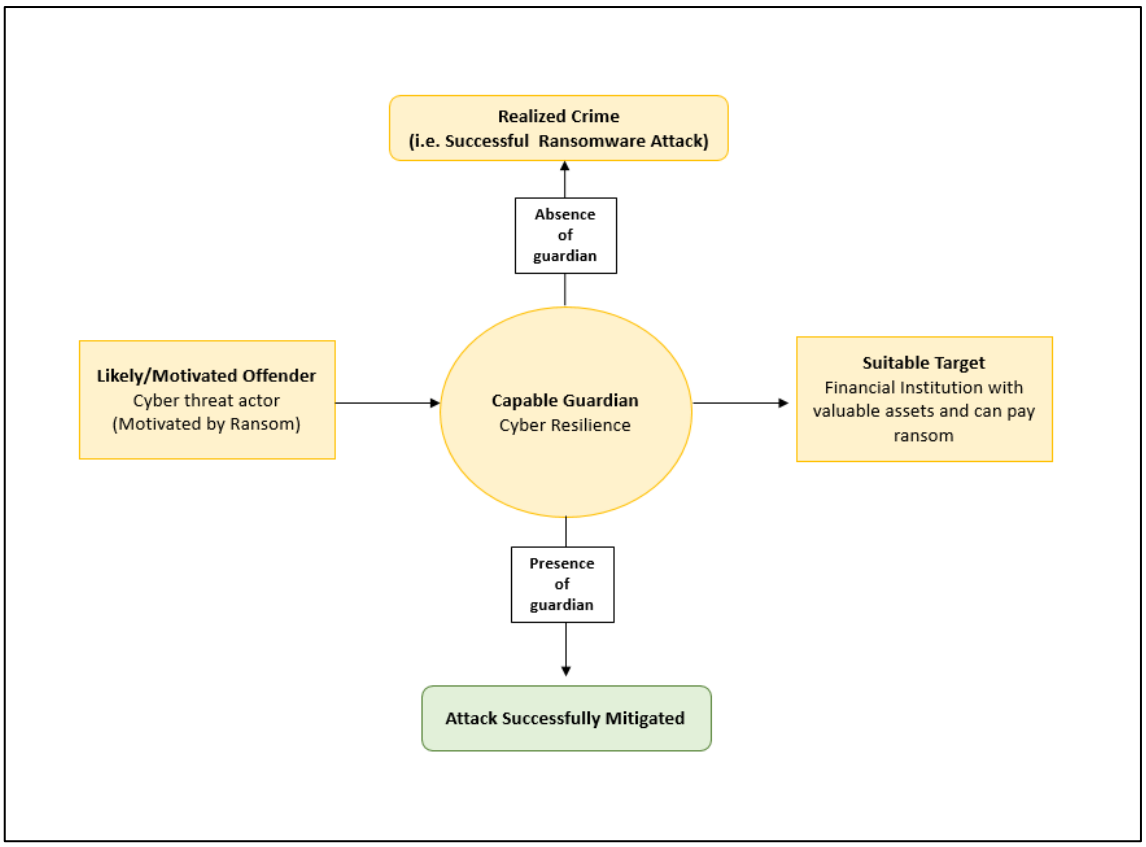


Figure 14 Application of Routine Activity Theory (Researcher own, 2022)

2.8.2 NIST Framework

To support this theory in evaluating the functionality of the research objectives, this study will also consider the security NIST Framework, previously referred to in the Introduction and Research Problem sections, focusing on the five core functions that are positioned to increase cyber resilience.



Figure 15 Five Core functions for effective Cybersecurity (Source: Hanacek, 2018)

The NIST framework is one that organisations align with as an industry best practice for their cybersecurity. The NIST framework is recommended to be used in conjunction with any implemented frameworks in organisations to complement rather than replace them (Almuhammadi & Alsaleh, 2017).

The NIST framework consists of five core functions, with the categories and sub-categories derived from various industry best practices, standards, and guidelines. The five core functions aim to offer a high-level and strategic view of an organisation's lifecycle in the management of cybersecurity risk (NIST, 2018).

The five core functions are described below. Important to note is that these functions are not prescribed to organisations but rather to offer a static end state for the organisation's cybersecurity programme.

Identify:

For an organisation to adequately put cyber-attack mitigation strategies in place, they would need to ensure that they have a full inventory of key elements within their business, such as critical information, company assets, and existing capabilities. The ‘identify’ function’s objective is to help guide organisations to identify and adequately manage their cybersecurity risk to systems, people, assets, people, data, and capabilities. Categories within this function include

asset management, business environment, governance, risk assessment, and risk management strategy (NIST, 2018).

Protect:

An organisation has a mandate to protect their critical infrastructure as well as to ensure that there is minimal impact in the event of a cyber-attack. The ‘protect’ function provides guidance to organisations on how to develop and implement appropriate safeguards for critical infrastructure. The categories of this function include identity management and access control; awareness and training; data security; information protection processes and procedures; maintenance; and protective technology (NIST, 2018).

Detect:

In a case of a cyber-attack, to potentially minimise the impact thereof, an organisation needs to be able to swiftly detect the activities of cybersecurity events. The ‘detect’ function assists organisations to timely discover cybersecurity events, where they can use various tools and techniques to achieve this. Categories of this function include anomalies and events; security continuous monitoring; and detection processes (NIST, 2018).

Respond:

Once a cybersecurity event has been detected, the cybersecurity team needs to be able to respond accordingly to minimise the impact of the attack. The ‘respond' function offers guidance on how organisations can develop and implement suitable actions and activities once a cybersecurity incident has been detected. Categories within this function include response planning, communications, analysis, mitigation, and improvements (NIST, 2018).

Recover:

In the unfortunate case of a successful cyber-attack or intrusion, an organisation will need to ensure that they are able to recover in a timely manner to avoid a severe and widespread impact on business and customers alike. The 'recover' function thus provides guidance around this in terms of how organisations can

develop and implement activities required to maintain resilience plans, including backing up critical systems and restoring any impacted capabilities and services. Categories within this function include recovery planning, improvements, and communications (NIST, 2018).

Furthermore, one would also need to factor in an assessment framework or method, which would help in assessing the effectiveness of the strategies selected to mitigate cyber-attacks. Having an assessment framework or method in place will assist management in basing their decisions on tested foundations and subsequently help them to outline and prioritise their investment strategy to improve their cyber resilience maturity level.

2.9 Research Propositions

Based on the literature review and in line with the research objectives, the following propositions are put forward:

2.9.1 Proposition one

Ransomware is prioritized as a top risk as threat actors' motivation is heightened to exploit financial institutions.

2.9.2 Proposition two

Components derived from the NIST framework (Identify, Protect, Detect, Respond and Recover) are key factors that influence cyber resiliency in financial organisations.

2.9.3 Proposition three

Senior management have a critical role in ensuring cyber resiliency in financial institutions.

2.9.4 Proposition four

Various methods and techniques can be employed to evaluate the cyber-resilience of an organisation.

2.10 Research Gaps

Through this literature review, there is an indication that the cyber-resiliency of South African financial institutions is not clearly defined or well documented in research. Additionally, there is a limitation in detailed exploration of various emerging threats including the use of Ransomware-as-a-Service or artificial intelligence, which may contribute to things to consider when formulating a mitigating strategy. When considering the aspects of management's role and decision-making, while the research indicates the importance of the role management plays in cybersecurity management, there is not a wide coverage on challenges that are faced by management in implementing cyber-resilience strategies. Additionally, to further enhance the practical application of remediation, the researcher was unable to find specific guidance on prioritization of remediation efforts when it comes to formulating a strategy to mitigate ransomware risks.

2.11 Conclusion:

Studies have indicated the rapid growth in cyber threats and the dynamic cyber landscape that many organisations grapple to keep up with. It is well noted that cyber-attacks have also increased specifically in financial institutions, where attacks have shifted from just attempts at extorting money from organisations to targeting the attractive exploitation of data housed in financial institutions. One cannot ignore the role that COVID-19 also played in accelerating the number of cyber-attacks. Organisations were forced to move most of their operations remotely, opening several vulnerabilities that cyber attackers took advantage of. Further to this, over the last few years, there has been a notable rise in

ransomware attacks on various organisations across the world. This has encouraged organisations to search for effective strategies to ensure safeguarding their critical assets and disruption of services. This is where cyber resilience strategies have been considered as a possible effective strategy to prevent and mitigate against ransomware attacks.

To help organisations improve their cyber resilience against cyber-attacks, they are encouraged to adopt various industry standards and frameworks and apply them in conjunction with their cybersecurity strategy for the best possible chance at mitigating cyber threats. This is supported by literature indicating that organisations may not be able to be completely cyber-secure; however, they can adopt adequate controls to strengthen their cyber resilience.

Additionally, for a cyber-resilient strategy to be effectively implemented, literature shows that senior management plays a crucial role in leading an organisation's education and training, effecting sufficient budgeting, and effectively influencing a cyber-secure culture across the organisation. This is done through awareness, effective communication to the board and rest of the organisation, as well as giving the IT teams on the ground the necessary support needed. Finally, the researcher identified the need for the evaluation of strategies, including cyber-resilience, to assess their effectiveness. Literature offers various frameworks and methods to assess the cyber-resilience of organisations to confirm the effectiveness of the strategy, rather than relying on untested controls.

3 Research Methodology

This chapter provides an outline of the research methodology that was applied in the study to answer the research questions outlined in Chapter 1.

The study investigates cyber-resilient strategies that financial institutions in South Africa can adopt to mitigate and respond to cyber-attacks, with a key focus on ransomware attacks. This section covers aspects of the conceptual framework, research design, data collection methods, sampling, the strategies, and approach for analysing the data, limitations and challenges experienced during the study, and ethical considerations. This chapter is closed off with a conclusion.

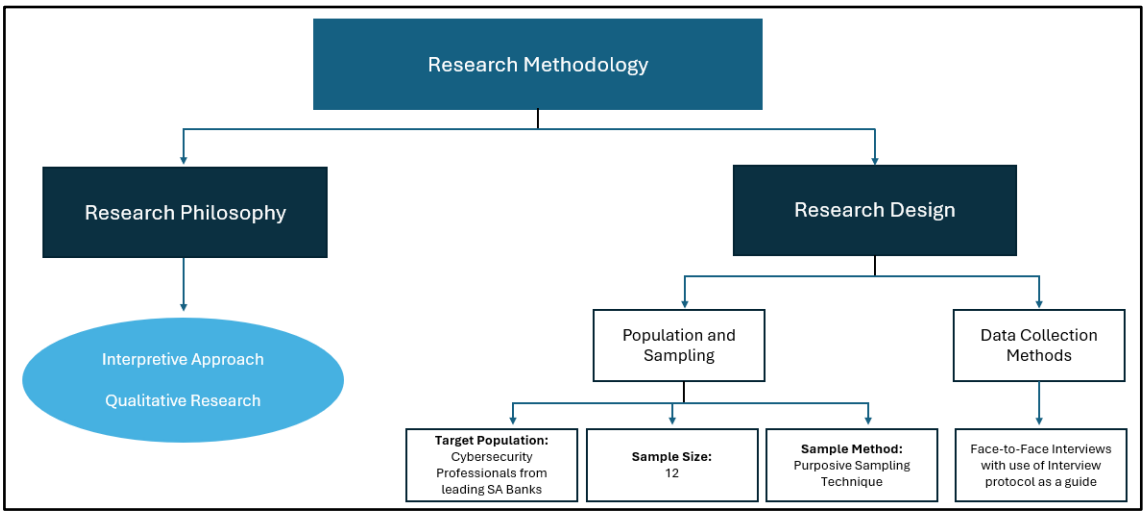


Figure 16 Diagrammatic Representation of Research Methodology

3.1 Conceptual Framework

To best achieve the research objectives, this study presents a conceptual framework that outlines the direction of the research and the relationships and variables to be considered in the study. See the figure below:

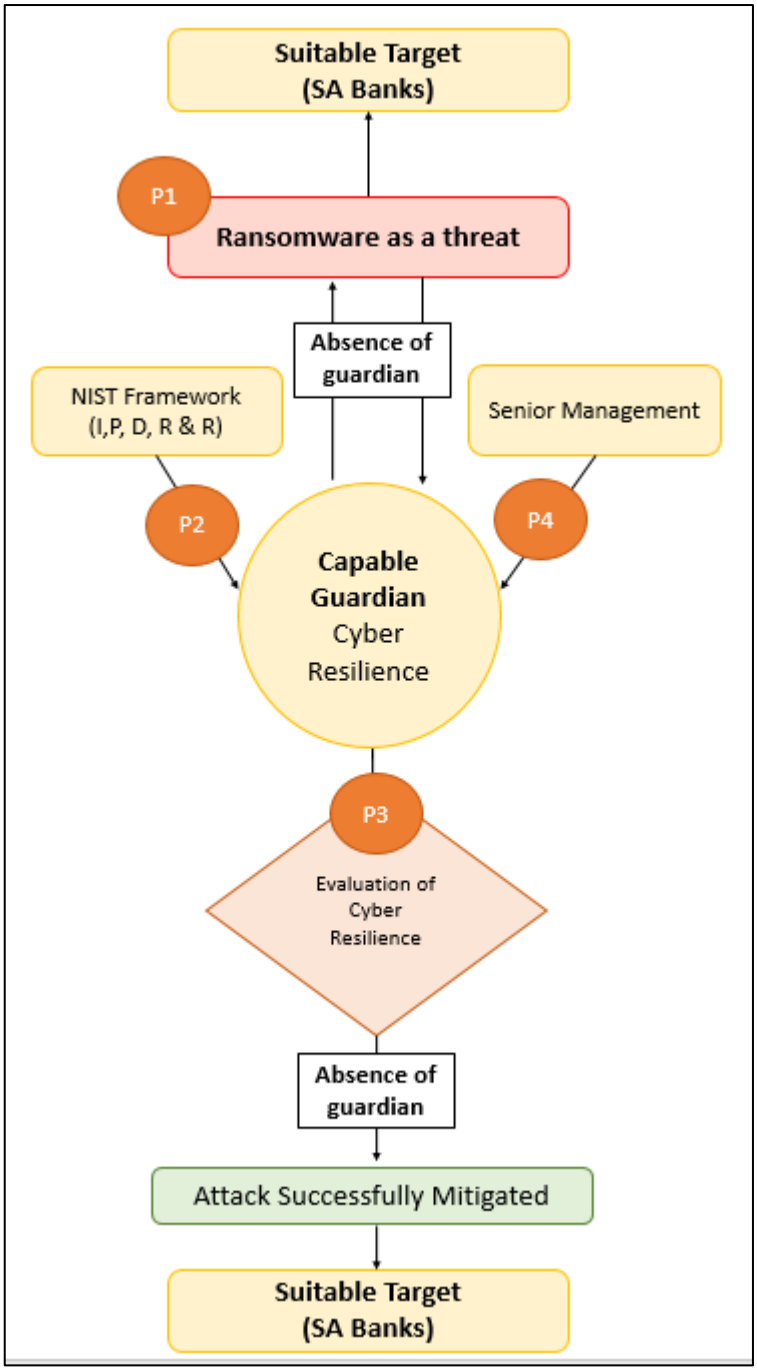


Figure 17 Adaptive Cyber Resilient Framework (Researcher own, 2023)

This conceptual view of the Adaptive Cyber Resilient Framework tests the cyber-resilience posture as a capable guardian of a said financial institution—a likely offender presented in an earlier RAT conceptualised model by the researcher. Using the NIST core functions (Identify, Protect, Detect, Respond, and Recover) and the role of senior management as a contributing factor to the resilience criterion, the model is able to provide a view of whether an employed cyber-

resilient strategy would be effective in mitigating a cyber-attack, with cyber-resiliency being assessed by the methods to evaluate cyber-resilience.

3.2 Research approach

For the purposes of this study, an interpretive approach is used. According to Clayton et al. (2018), the interpretive approach is deeply rooted in the human sciences, centred around how human beings make sense of their subjective reality and attach meaning to it. This approach is noted to be frequently used in qualitative research because of its nature to enable researchers to investigate complex studies by gathering insights into their participants' views and experiences, as well as associate meanings with occurrences (Antwi et al., 2015).

In the context of the research objectives, this approach assists the researcher in understanding the various approaches taken by cybersecurity personnel at various management levels to ensure cyber resilience for their respective organisations.

3.3 Research design

This study adopts a qualitative method. The aim of the qualitative research method is to understand and investigate a variety of experiences, viewpoints, and behaviours or actions of people or groups (Mohajan, 2018). Tenny et al. (2022) describe that, at its core, qualitative research is focused on asking open-ended questions where the responses cannot easily be put into numbers or linear explanations. This research method offers flexibility in unhurried interactions with participants, allowing the researcher to capture detailed experiences much more than a simple collection of statistical analysis (Carter & Henderson, 2005). To support this research method, methods, and techniques such as interviews, focus groups, case studies, and observations are used to achieve the objectives of qualitative research (Yates & Leggett, 2016).

For this study, the researcher deems qualitative research an appropriate method to gain detailed descriptions and understanding of cyber resilience within financial services when it comes to ransomware cyberattacks.

3.4 Data Collection Methods

For comprehensive and in-depth information gathering, this study uses a primary data collection method. Hox & Boeije (2005) define primary data as “original data collected for a specific research goal”, and secondary data as “data originally collected for a different purpose and reused for another research question”. The advantage of using primary data as a data collection method is that the researcher has a level of control over who will participate as well as an independent direction in terms of the research design and data collection thereof. To corroborate the primary data, data collected from the secondary collection method can be used to enrich the research where there may have been limited available research or data from the primary data (Hox & Boeije, 2005). For this study, the researcher considered a literature review to corroborate the primary data collected.

The primary data was collected using the methods of semi-structured interviews to encourage participants to elaborate on their opinions as well as to give the researcher an opportunity to ask any clarifying questions.

3.5 Population and sample

This section of the study outlines the sampling method that was used along with the targeted population of the participants.

3.5.1 Population

A target population of a research project is defined as a defined population from which the sample has been carefully selected (Banerjee & Chaudhury, 2012). With the objective of investigating cyber-resilience as a strategy to mitigate ransomware cyber-attacks in South Africa, the target population is cybersecurity professionals from the leading South African banks (PWC, 2023).

The study targeted three respondents from the cybersecurity departments of each of the four leading traditional banks to explore and understand their cyber resilience posture when it comes to ransomware cyber-attacks, as well as gather the various opinions of what the South African banks still need to get in place in order to have sufficient cyber resilience against ransomware cyber-attacks. The total targeted number of participants was therefore, 12.

3.5.2 Sample

A 'sample' is defined as ‘a subset of the population, selected to be representative of the larger population (Acharya et al., 2013). Taking into consideration the chosen data collection method, conducting interviews can become time-consuming as well as costly if there are any incentives offered to participants to take part in the study; thus, having a sample can reduce the research time, effort, and associated costs (Acharya et al., 2013). The study is focused on assessing cyber resilience as a strategy to mitigate ransomware cyber-attacks within their respective organisations; therefore, the sample that was selected was focused on professionals who work in and have knowledge and experience within the field of cybersecurity. The participants that agreed to be part of the study fulfilled roles including IT Risk Management, Cybersecurity Incident Responder, Cybersecurity Consultant, Cybersecurity Office Strategy Lead, and IT Security Governance, all of which work in one of the four major South African banks.

3.5.3 Sampling method

Taking into consideration the scarcity of cybersecurity professionals (Lake, 2022), the study made use of a purposive sampling technique. As per the definition covered by Acharya et al. (2013), the purposive sampling technique is when a researcher would use their discretion based on prior knowledge or expertise to select a sample that would be most useful to the research. Having a purposive sample for this study enabled more cybersecurity-focused feedback in answering the research questions.

3.6 The Research Instrument

An interview protocol was developed that encompassed all the questions to be posed. It emerged from the literature review.

The interview protocol was subsequently used as a guide during the interviews, with the intent of focusing the line of thoughts and tracking which other questions may have been covered. The interview protocol also assisted the researcher in keeping the various interviews in a similar format and structure.

The interview questions were designed to adequately respond to the outlined research topic and questions alike and can be retrofitted through the conceptual framework positioned in Chapter 2.

Prior to conducting the semi-structured interviews, the researcher conducted a peer review of the interview questions with three academics to ascertain that the drafted questions were of high quality and would enable the researcher to obtain the best possible responses in line with the study. The feedback collected from the peer review of the interview questions was duly incorporated into the final interview protocol.

As part of a pre-test, the researcher conducted a ‘pilot interview” to further identify any areas of improvement in the interview protocol and questions themselves, as well as highlight any improvisation. The final interview protocol that was used can be found in Appendix C.

3.7 Procedure for data collection

The selected data collection instrument for this study was a semi-structured interview, which required targeted participants (i.e., participants working in a South African bank within a cybersecurity or information security department) to obtain the objectives of this study.

The following procedure was followed for data collection:

Identifying participants

The researcher first identified the primary financial institutions and participants within prior knowledge of the researcher, and using the snowball sampling technique, identified further participants with similar experience and knowledge within the targeted industry. The researcher made initial contact with each of the potential participants to invite them to participate through an informal platform including text and WhatsApp, providing each participant with a high-level description of the intention of the study. The research also used the informal platform to get more details about the participants, including their experiences, to ascertain if they were best suited to participate in the study.

Contacting participants:

Once the potential participants were identified, the researcher contacted each participant via email, sharing the research objectives and using the opportunity to pursue voluntary participation and informed consent. The researcher further asked the participants to communicate their availability so interviews could be conducted.

The targeted participants were sent a 'request for participation' letter where the outline of the study was shared as well as to obtain particulars of the participants with regards to the role they fulfil within the cybersecurity field and request that they sign an informed consent form consenting to participate in the research study. Subsequently, a semi-structured interview was conducted with each participant who volunteered to participate in the study to get an in-depth understanding of their respective cyber resilience stance. The researcher managed to get representation from all four major South African banks to participate, with a total of eleven participants taking part in the study.

Conducting interviews:

Once the participants had agreed to participate in the study and completed all necessary documentation (i.e., consent forms), the researcher scheduled interviews in the format and time that accommodated the participants. The primary data was subsequently collected through semi-structured interviews,

both face-to-face and online. When conducting interviews, the researcher voiced over the objectives of the study once again and obtained permissions for recording and transcribing prior to the interview. The researcher then conducted a question-and-answer session with the participant, also taking any additional notes using a notebook, which was considered raw data and used as part of the analysis.

Addressing biases during interviews:

Interviews are a fundamental qualitative research method, but their reliability hinges on minimizing bias. To achieve this, the researcher primarily ensured that the designing of the questions seek factual information rather than opinions, encouraging the respondents to focus on objective data. The consistency in questioning during the interviews also played a pivot role in minimizing biasness, for this study researcher made use of a standardised interview protocol to guide the line of question and ensure uniformity across interviews. A neutral tone is also maintained throughout all interviews to prevent inadvertent influence.

3.8 Data analysis and interpretation

This section describes the process that the researcher followed to analyse the data collected during the semi-structured interviews. While the collected data forms the backbone of research, correctly analysing the collected data is an integral part of the research, assisting to interpret any potential flaws as well as providing a collective of insights (Bhatia, 2017).

For this study, the researcher used thematic analysis, which is an analysis method usually applied to qualitative data. This method was applied to the data collected in the study by identifying common themes, topics, ideas, and patterns that may come up frequently (Caulfield, 2022).

Below is an outline of the data analysis strategy and interpretation that were employed:

Semi-structured Interviews:

- **Gathering and Collecting data**

Each of the interviews were recorded by the researcher and transcribed with permission received from each participant. Recording and transcribing each of the interviews allowed the researcher to be able to revisit the interviews and listen to each response to ensure that it was captured correctly. The researcher further underwent an edit of the transcription to ensure that it was correctly documented. To ensure tracking of each completed interview, the researcher used an Excel spreadsheet to document interviews completed, with raw summary notes of insights received per participant as well as any additional notes pertaining to the interview itself. The researcher also used a number and alphabet representation for each participant, which was later used as a reference to maintain the confidentiality and anonymity of the participants as well as the organisations they work for.

- **Organizing and connecting data**

Leveraging the Excel spreadsheet that the researcher used to track interviews, the researcher organised the data according to responses received from each participant. Using the transcripts, the researcher created a tab on the spreadsheet for each participant and copied across responses per question and later grouped responses per question, where coding would then be derived.

- **Coding/Categories**

Bailey (2007) describes the process of coding assigning specific codes, words, or phrases to easily identify topics or themes which can later be categorized, grouped, or linked.

Using the final transcriptions and notes taken during the interviews, the interviewer proceeded to perform “coding” on the raw data documented in the spreadsheet per question. The process for coding included reading the data and identifying potential themes emerging from the datasets, followed by using different highlighting colours to identify similarities. This was an iterative process which led to the revision of themes and later assisted with improving accuracy and applying the coding consistently. Once the coding had been completed, the various responses now categorized per theme were exported into a separate spreadsheet for ease of reference.

- **Analysing for insights**

Bailey (2007) describes the process of coding, assigning specific codes, words, or phrases to easily identify topics or themes that can later be categorised, grouped, or linked.

Using the final transcriptions and notes taken during the interviews, the interviewer proceeded to perform “coding” on the raw data documented in the spreadsheet per question. The process for coding included reading the data and identifying potential themes emerging from the datasets, followed by using different highlighting colours to identify similarities. This iterative process that led to the revision of themes and later assisted with improving accuracy and applying the coding consistently. Once the coding had been completed, the various responses, now categorised per theme, were exported into a separate spreadsheet for ease of reference.

- **Reporting of insights**

The last step in the data analysis component included documenting the findings and linking insights to the research questions, as well as the literature review. The objective of the final report of insights is to provide a perspective on the use of cyber resilience as a strategy to mitigate ransomware cyber-attacks, specifically through the lens of banks in a South African context.

3.9 Limitations of the study

When conducting a research study, it is prudent to note down any limitations and challenges that the study may encounter.

The researcher initially envisioned having a balanced and equal number of participants from each identified organisation, i.e., three (3) participants per organisation. While invitations for participation were sent to various potential participants in each organisation, some of the participants declined to participate, and others struggled to find a convenient time to participate in the interview. On availability, of the eleven (11) interviews, five had to be rescheduled at least once, with two (2) requesting a change of date and time on the day of the interview.

This impacted the planned time for completing the interviews, subsequently causing delays in the progress of the project.

Ten (10) out of the eleven (11) interviews were conducted using Microsoft Teams, which also presented a number of challenges, including two (2) of the interviews experiencing issues surrounding load shedding impacting the network and resulting in further rescheduling of the interviews.

An additional challenge for the researcher was also presented in the form of personal bias, where the researcher works for a financial institution within the cybersecurity field and constantly needs to check and maintain objectivity when conducting the study as well as analysing the collected data.

3.10 Quality Assurance

When conducting a study, it is important to ensure that the quality, reliability, and integrity of the data are maintained throughout the project. Quality assurance in a research project are strategies a researcher puts in place to ensure the quality, reliability, and integrity of the data. This is helpful to ensure that there is adequate compliance through every stage of the study as well as assists in evaluating the researcher's own research and the management of the data to produce the best possible results (Wisconsin-Madison, 2020).

In this section, the credibility of the study will be discussed, as well as the triangulation method that will be used to ensure the quality assurance of the project.

3.10.1 Credibility

The credibility of a study aims to establish confidence in the data, where the views and experiences of the participants are recognisable within the study (Patton, 1999). According to Patton (1999), the credibility of the study has three distinct elements, which include:

- The techniques and methods that a researcher uses to gather high-quality data that is deemed to be well analysed with evidence of validity, reliability, and triangulation.

- The credibility of the researcher, which may include previous experiences, training, status.
- The overall philosophical belief of naturalistic inquiry.

For this study, the researcher followed the following steps to ensure that the credibility of the study was maintained:

- **Reflexivity journal** – The researcher kept and maintained a reflexivity journal where all notes regarding the progress of the research project were documented. This included, but was not limited to, ideas, emerging themes stemming from literature, reflections on conversations on related topics and ideas linked to the study, as well as reflections from each interview. The researcher also made sure to document a summary of each interview at the end of the interview to note how the general interview went as well as any key insights worth noting so they could be revisited during the analysis stage.

- **Peer-to-peer review** – Prior to finalising the interview questions, the researcher conducted a peer-to-peer review of the interview questions. The objective was to establish whether the flow of the question made sense, to evaluate if the questions were phrased in a manner to sufficiently help gather quality data, and to get a sense of any additional opinions that will assist in putting together a quality report.

- **Peer Debriefing** – The researcher conducted a pilot interview to evaluate the validity of the final interview questions as well as the flow of the interview. Post-pilot interview, the researcher conducted a debrief to get feedback on the overall flow and quality of the interview, as well as probing the quality of the questions and the data the peer deems can be derived from the set of questions asked. The researcher also engages peers currently completing a similar qualification on emerging insights obtained from literature and observed industry trends to ascertain whether they would be worth incorporating into the research paper.

- **Strategies of guaranteeing trustworthiness in participants** – The researcher used snowball sampling when selecting participants, which included a step to probe the level of experience the referred participant has within the cybersecurity field, so the researcher gained a level of confidence in the responses received from each participant. Each of the participants was also required to complete a consent form to participate in the study.

3.10.2 Dependability

The dependability of a study refers to a researcher maintaining the consistency and reliability of the research findings and the methodology followed. An independent researcher following the same outlined design, methodology, implementation, analysis, etc. with the same participants would be able to reach the same or comparable results. It is therefore important for the researcher to ensure that there is adequate documentation throughout each research stage, which would serve as an audit trail for the research project (Moon et al., 2016). For this study, the researcher will keep a reflexivity journal and field notes during interviews with participants to keep track of the various observations that may not be reflected in the interview answers.

3.10.3 Triangulation

A method of choice for this study to ensure quality assurance is triangulation. The concept of triangulation is used to check and establish the validity of the research findings, being able to prove that the qualitative evaluation findings are valid and of decent quality (Guion, 2002).

There are five (5) types of triangulations that can be applied in a qualitative study, according to Guion (2002). The five types of triangulations are defined in Table 2 below:

Table 4 Types of Triangulations (Source: Guion (2002))

Type	Definition
Data Triangulation	Data triangulation involves the use of different sources of data/information.
Theory Triangulation	Involves the use of multiple professional perspectives to interpret a single set of data/information.
Investigator Triangulation	Involves using several different investigators/evaluators in an evaluation project.
Methodology Triangulation	Involves the use of multiple qualitative and/or quantitative methods to study the program.
Environmental Triangulation	This type of triangulation involves the use of different locations, settings and other key factors related to the environment in which the study took place, such as time of the day, day of the week or season of the year

Taking into consideration the nature of this study, this study will adopt data triangulation. The chosen triangulation type was implemented by identifying the different stakeholders in terms of their role in cybersecurity within their respective organisations. Each of these stakeholder groups was interviewed, and as part of the analysis, the researcher looked for outcomes that were agreed upon by all the stakeholder groups across the various organisations. Where the same or similar outcome was observed, the outcome was ranked as likely true.

3.11 Demographic profile of respondents

The data collected is from eleven (11) interviews, which were conducted with participants from four South African banks. All persons that participated in the study are domiciled in South Africa, consisting of six (6) males and five (5) females. The level of seniority of the participants ranged from middle management to supervisory management within their respective cybersecurity departments. The role designations of the participants ranged across risk management, governance, cybersecurity consultant, incident responder, and security strategist. The requirement outlined for participation was based on the participants being well versed in the field of cybersecurity and knowledgeable about ransomware as an attack vector.

3.12 Ethical considerations

When conducting this study, it was important to ensure that ethics were considered to protect the rights of the participants, enhance the research validity, and maintain the integrity of the study throughout (Bhandari, 2021). Due to the topic of this study, the confidentiality of the participants is a critical consideration, as the research results pointing to a specific organisation could result in an unfavourable consequence, i.e., the highlighting of cyber-resilient gaps specific to an organisation. The study therefore offered confidentiality to the participants by anonymizing personally identifiable information that could be linked to the participant or the organisation they work for. Where the participant needed to provide personal information, even if it were only for the benefit of the researcher's analysis, the handling of this data was outlined and explained to the participants so that they were aware of how their personal information would be managed.

In line with respecting participants and organisations' boundaries, the design of the interview questions ensured that they followed an ethical thread and were not intrusive to the participants.

In a case where a participant required the researcher to sign a non-disclosure form, the researcher was open to adhering to the request, with a clear

understanding of which information can be included in the study report and which can only be used for context or informational purposes. For this study, however, such a request was not made.

The study also ensured that participants were given the freedom of participation, where they were offered to opt in or opt out of the study at any point. Participants were given informed consent, where the purpose, benefits, and any related risks were shared upfront. The researcher also requested permission for recording and transcription when conducting interviews; participants were also given a choice to opt in or out during this process as well.

All the data collected from the participants was carefully managed and stored on a password-protected computer. Where sensitive data may need to be sent via email, the researcher ensures that the data is locked with a password.

Adhering to WITS guidelines, the researcher submitted an ethics application for approval prior to conducting the research to ensure that all ethical considerations were accounted for in this study.

3.13 Conclusion

In this chapter, the researcher discussed the research method employed in the study, following a qualitative research method to help the researcher gain insights from individuals who work in the field of cybersecurity and in financial institutions without having to expose sensitive details of organisations. For the research approach, the researcher adopted the interpretive approach.

To cover the four major banks in South Africa, the researcher targeted three respondents from cybersecurity departments per bank. The objective was to explore and understand their cyber resilience posture when it comes to ransomware cyber-attacks, as well as gather the various opinions of what the South African banks still need to get in place to have sufficient cyber resilience against ransomware cyber-attacks. In total, the targeted number of respondents was 12, and the researcher was able to finally get eleven participants to partake in the study after employing a snowball method to identify suitable participants.

To collect data, the researcher used semi-structured interviews, which were conducted mostly remotely and a few face-to-face, and a recording as well as a transcription for all the interviews was done for each of the interviews. The recording and transcriptions were later used as part of the data analysis, where the researcher followed a thematic analysis method to identify common themes, topics, ideas, and patterns that came up frequently during the study.

This chapter further discusses the techniques followed to ensure quality assurance by looking at the credibility aspects employed during the study and the use of triangulation to verify quality assurance. The ethical considerations and challenges experienced by the researcher are also discussed in this chapter.

4 Research Findings

4.1 Introduction

This chapter presents findings from the research conducted on South African banks' cyber resilience strategies against ransomware attacks. The data for this study was collected through eleven semi-structured interviews with participants from the four South African banks, where each participant voluntarily participated by answering structured interview questions in response to the research topic. The level of seniority of the participants ranged from middle management to supervisory management within their respective cybersecurity departments. The role designations of the participants ranged across risk management, governance, cybersecurity consultant, incident responder, and security strategist. Each interview was recorded, and a transcription was downloaded from the recording. After this, the researcher then cleaned up the raw data produced from the automated transcriptions to place it into a readable format, followed by compiling a response summary from each participant as an initial step in understanding the data collected.

The basis of the interview questions was founded on the research objectives as outlined in Chapter 1:

- Assess the level of concern and prioritisation that organisations have for ransomware cyber-attacks.

- Investigate the key influences that contribute to the cyber-resilient posture of an organisation against ransomware attacks.

- Assess the role and influence of senior management in influencing the resilient posture against ransomware cyber-attacks.

- Investigate how organisations can evaluate the maturity and effectiveness of cyber resilience as a mitigating strategy.

As the interviews were conducted anonymously due to the nature of the sensitivity of responses potentially being linked to specific organisations that

could lead to vulnerabilities being exploited or targets for the organisation, the agreement between the researcher and participants was to keep all responses and demographic information confidential.

Explanatory code:

For the purposes of this study and the narration of the responses, the role designations have been numbered chronologically: risk managers equate to 1, incident responders equate to 2, governance officers equate to 3, security consultants equate to 4, and CSO strategists equate to 5. The participant code is arranged alphabetically in the order that they were interviewed. When a participant is referenced in the narration, a combination of the role designation and participant code is used as follows: “1A”, denoting the first participant interviewed who is a risk manager.

Role Designation	Participant Code	Participant Reference
(1) Risk Managers	A, B, J, K	1A, 1B, 1J, 1K
(2) Incident Responder	C, I	2C, 2I
(3) Governance Officer	D	3D
(4) Security Consultant	E, F, G	4E, 4F, 4G
(5) CSO Strategist	H	5H

Table 5 Information of participants

The findings presented are in line with the propositions and theoretical framework outlined in Chapter 2 and are presented in a narrative format, where verbatim extracts from the interviews are indicated using quotation marks. To ensure easier and clearer reading of the responses, the researcher removed repeated

words and filler words during the examination of the transcripts. The researcher also makes exploratory comments to examine emerging themes that are further discussed in detail in Chapter 5.

Interview Findings

4.2 Research objective 1: Assess the level of concern and prioritization that organisations have on ransomware cyber-attacks.

Research objective one relates to understanding whether the cybersecurity strategies within financial institutions prioritise the rising threat of ransomware.

In response to the question on the level of concern that South African banks have about ransomware attacks, all eleven respondents indicated that their respective organisations considered this type of attack a top risk. Two of the respondents indicated that the risk is considered a top priority risk, further highlighting that there are dedicated programmes to ensure that there is sufficient protection and that they can limit exposure to risk. Three of the respondents explain that financial institutions have become a prime target of ransomware, as the impact on their operations, their CIA, and their bottom line would be exceptional. Responder 4F indicates that one simply cannot ignore ransomware.

> “I mean you can't ignore ransomware if it hits you, you will know and everybody will know, you just can't hide it like you can hide various other types of malware or types of cyber-attacks, but ransomware is definitely guaranteed to have an impact on your operations and ultimately potentially your bottom line, so should be taking care and should be considered as a top risk by management." (4F)

One respondent, however, provided a contrasting view that South African banks have a big budget, high-quality and latest technologies, and the resources to defend themselves against large-scale ransomware attacks; however, this may not be the case with their third-party service providers. Consequently, the banking sector has not been a big target, but rather targets seem to be more third parties, where respondent 2C highlighted that most previous ransomware incidents were

because of third parties being compromised and there were traces of lateral network movement attempts into the banks' networks.

While the nine respondents focused on external threats, one respondent leaned towards encouraging organisations to invest more in increasing protection from insider threats. Respondent 1A highlighted that an insider threat is likely to do more damage than an external threat actor would be able to.

"The major risk is the insider threat which we need to look into because of most people who work inside are familiar with the processes and the technology that we are using. Then they know the loopholes that we might have, you know, or they can connive with someone who works in the security team. So, when you look at the threat landscape for me, I think in the South African banking industry, it is more of an insider threat that we need to look into rather than external threat. By saying that I am not saying that we should overlook the outside part of it, but I'm saying that we should tighten security both inside and outside, especially with the focus of the insider threat because of that's where the people are implementing the systems. They know the gaps and they can take advantage of that." (1A)

Additionally, one respondent highlighted that the cyber threat landscape has evolved, highlighting the ease of deploying ransomware even though the attacker may not have high technical skills, due to the introduction of ransomware-as-a-service (RaaS).

"I think the last thing I think one of the main reasons that drove the increase is Ransomware-as-a-service. So you don't have to be a technically skilled to launch a ransomware attack. You can actually buy the service in the dock whip which is really why we see such an increase." (1B)

The consensus that filtered through the responses was that South African banks have a responsibility to ensure that there is adequate cybersecurity to ensure that the "crown jewels" are well protected from such an attack. It also emerged that banks have a mandate to ensure service availability, integrity of data, and the

confidentiality of customer information, which are all aspects that ransomware has the power to compromise.

"The banking sector deals with people's information and money. If anything hits that and you don't have access to your files that means people can't do transactions. And I mean in this economy your money is very important. You worry so much about it like I'd rather lose an e-mail, or you know something else. But if I don't have access to my money then I start freaking out." (G4)

4.3 Research objective 2: Investigate the key influences that contribute to a cyber-resilient posture of an organisation against ransomware attacks.

Research objective two relates to determining key influences that would contribute to cyber-resilience. In responding to which key influences contribute to cyber-resiliency, five of the respondents highlighted the importance of being able to adequately identify and be aware of the organisation's critical assets. The one respondent highlighted that when designing a cyber-resilience strategy, understanding what assets the organisation has and what their value is becomes important in determining whether to place more focus on protection or recovery aspects. When referring to value, it is also key to be aware of the value of the assets for the cybercriminal and not just for the organisation. Overall, this will also assist in determining the insurance amounts. Subsequently, this encourages organisations to be aware of the threat landscape so that they can adequately adjust what needs to be adjusted to maintain adequate protection. One respondent made a note that in organisations identifying their assets, it can help inform which systems to prioritise backing up and the sequence in which they would need to restore in a case of an attack.

“One of the things that I find is a challenge for organizations is not everybody understands what they have or know what they have. Or sometimes they know it works, but they don't necessarily understand how it works. So you need to first understand your environment and after that start working on that and prioritizing this crown jewels you need to focus on what is the most important application and work from that. And the one application that you can't live without and start

working from there because not every organization is going to be able to replicate the whole data center.” (E4)

As part of understanding the internal environment and the external threat landscape, three of the respondents encouraged organisations to run risk assessments and threat scenarios to help them understand where their biggest risks lie. Running risk assessment assists organisations to identify trends and can effectively plan and implement correct controls to increase cyber-resiliency.

Bringing in the component of the ability to protect, six respondents shared various aspects of how organisations can ensure that there is adequate protection at all levels. Two respondents explain that protection mechanisms span from the whole organisation being risk-aware right through to ensuring that backups are in place and organisational data is protected even in the event of an attack. The protection aspects highlighted also include the hardening of the environment and taking guidance from best practices. Vulnerability management, anti-virus updates, regular patching, and the management of system and service accounts also emerged as protection mechanisms that increase cyber-resilience for an organisation. The effective management of privileged access emerged as an element that organisations need to pay attention to, as three of the respondents raised concern that it is an area that organisations may still fall short on and can certainly increase the risk of insider threats. Building human resilience emerged as a top priority, with eight of the respondents highlighting the importance of staff training on cybersecurity. Respondent 4G encourages that organisations spend time conducting phishing campaigns and simulations for staff members to be able to easily identify potential threats.

Two of the respondents further highlighted the ability to detect as one of the critical factors that contribute to successful cyber resilience. Respondent 4E shares that many organisations sometimes only find out about a cyber-incident once it happens, at times even a few weeks after the incident has occurred,

learning about it from platforms like the dark web. It emerged that organisations are encouraged to invest in detection tools, leveraging artificial intelligence technologies to assist in rapid detection of malicious traffic or malware in the network, as well as be able to identify malicious patterns and alert incident responders.

According to seven respondents, the ability to respond and recover emerges as one of the key factors to be considered by organisations to ensure cyber-resiliency. All eleven respondents agreed that organisations cannot fully protect themselves from cyber-attacks, thus, a response and recovery capability is a key factor in ensuring cyber-resilience. Seven of the respondents discuss the importance of having offline backups where the organisation can restore from in a case where their data is being held at ransom. Respondent 2C explains that organisations also need to have the right network architecture, with segmentation topology in place to reduce blast radius and plan an effective response for the various components of the network. Disaster recovery is encouraged by seven of the respondents, highlighting that planning for an attack through various DR simulations will help organisations rapidly respond and recover to normal business operations. As part of planning for responses and recovery, respondent 2I explains the importance of rapid decision-making. Organisations that are agile and do not depend on senior management to proceed with an incident response stand a better chance to maintain business continuity, as decisions as extreme as disconnecting the network during business hours to reduce impact are not stifled by CIOs, who may not understand the level of impact malware will have once it spreads.

“And very critical and I mean it's probably one of the most critical components is does your incident response team have the correct mandate within your organization to be able to the respond when that incident happens and be able to make all the decisions that are required to be able to safeguard your organization. Even if it does come down to making decisions of disconnecting systems during business hours and impacting business directly by the decision that they make at that moment. It might sound controversial, but because the ransomware would create impact, but the thing of taking certain systems offline

so that they don't get infected safeguards in a better way so that your response time of being offline and being able to restore your systems will be faster if they do take those hard decisions at that moment, like patting lines between data centers, removing communication between two data centers because if the infection is only in one data center, you cut the connection between the two data centers. You might create business impact, but you're safeguarding an entire data center at the mode. And the incident responder should be able to make that call with within minutes after making the call, be able to have that done, not sit in meetings or calls with executives in the organization to be able to make that decision or their method at the moment or to give them the green light for it, because by that time, the ransomware can already be moving into the secondary data center." (2I)

4.4 Research objective 3: Assess the role and influence of senior management in influencing the resilient posture against ransomware cyber-attacks.

Research objective three relates to assessing the role and influence that leaders, specifically senior management, play in influencing the cyber-resilience posture against ransomware attacks. Four of the respondents shared views on the importance of senior management being aware of associated risks and aware of the fast-changing threat landscape. They highlighted that because senior management makes the key decisions for the organisation, they need to have a good understanding of the threat landscape so they can ask the right questions and support cybersecurity initiatives. An emerging theme on the overall accountability of cyber-resiliency was noted as two of the respondents raised the overall role and accountability that senior management needs to take. This was contrasted by views from eight respondents who leaned towards accountability being integrated and shared with the rest of the business rather than being put on the CISO. One respondent supported this by highlighting that ransomware attacks do not only impact parts of the business but potentially the entire network, which would disrupt all business operations. It is not an IT or CSO problem, but

a risk that all business leaders need to be concerned about. Respondent 1B supports this notion, encouraging cyber-resilience to be built into the business strategy so that it does not become an afterthought.

“I really think it's a total organization commitment and it shouldn't be left to one set of stakeholders. However, they really need to understand the risks that are being reported to them. And the key is just to implement and make sure that all controls and tools that are required to remain resilient are in place and are operating as they should.” (3D)

In line with integrating cyber-resilience with the rest of the business, responder 4F brought up the challenge that organisations that keep cybersecurity initiatives separate from the rest of the business run at risk of not understanding the true impact that a ransomware attack would have on business operations. In the event of an attack, many parts of the business may not know their role in the response to the incident.

“I think there is what I say things get lost in translation. We speak tech language to business people and these people don’t always understand the tech language. So sometimes I would call it and say we need an API to translate the language to the guys to say this is what I mean when I say this 200 critical vulnerabilities. These people don't care about numbers like those. They care about the business exists to make money. Tell us how much you're gonna use. Tell us how much these things gonna impact us. And then when you've got that translation in place and it's properly understood by management, I've seen that the improvement actually happens when that is being translated to say this is what I mean as a CIO or a CISO.” (4F)

“In a case of an incident, to ensure that there is never a misconception around the exposure at any given point of time. To be able to give all of the support that's required, the understanding to the board of where you are and what needs to still be in place and what needs to go into the organization to be able to be resilient against something like this and also the full buy in from them to be able to support downwards in the organizations as well. So that if staff

members or teams comes with plans or stuff that they are able to be resilient, to support that with immediate effect." (2I)

"Lots of CISOs are very technical, but they also need to you know, be aligned to the business, because ultimately everything that we do needs to be aligned to business objectives. I know usually it's sometimes, the organizations CISOs don't really have a seat at the table as such. You know, they're reporting to the CIO and basically they don't have that forefront, you know in terms of that executive committees. I think it's obviously different for every organization, but I think that would be a critical step in terms of, you know getting that knowledge and obviously connecting the business with basically the cyber security activities." (1K)

Five respondents raised a key consideration around how senior management needs to prioritise cyber-resiliency within their business. Some of the views include ensuring that cyber resilience is flagged as a business risk rather than an IT or CSO risk. The respondents highlighted that when cyber-resilience initiatives are prioritised, senior management will ensure that there are adequate resources and skills development so that the teams are equipped to respond to attacks. Additionally, prioritising cyber-resilience will encourage sufficient budget and investment in technologies that can support cyber-resilience. Ransomware being considered a top risk will also get sufficient airtime in senior management meetings, inherently preparing the leadership to keep it top of mind as part of their business operations. Respondent 3D showed concern that SA banks may be needing a wake-up call as, while there is a lot of preparation underway on the prevention of ransomware, none of the main banks have suffered successful ransomware and may tend to relax in some instances, forgetting that there are zero-day attacks to be considered.

The researcher also took note of an emerging theme on senior management participating in simulations, where three of the respondents highlighted the importance of senior management participating in simulations.

“When we run this phishing simulations as well, they are specific targets especially for rent somewhere where they target the C level because they have the highest access you know I mean they sign off on the money they sign off on you know what needs to be done. So, they need to be aware, and they need to push it down.” (4G)

“I think it’s making sure that they make the time to exercise and understand the impact of specific scenarios. One thing we're very fortunate to is that our executive sees the value of simulation. Senior management need to get exposed to the impact into the technicalities of this, necessarily that they would solve it technically, but they need to get exposure to it.” (2C)

Simulations strongly help teams be better prepared for eventualities. One respondent highlighted that senior management can be a blocker in the case of an incident, where they may not necessarily understand the level of impact one particular risk carries for the entire organisation. Having the correct support from senior management therefore becomes critical for incident responses.

Lastly, the responsibility of encouraging a cyber-resilient culture across the organisation and ensuring that there are sufficient resources emerged, as six of the respondents supported the idea that senior management should be responsible for influencing and encouraging a cyber-resilient culture as well as ensuring that there are sufficient resources to support cyber-resiliency.

“…And also setting the culture. You know that we've got a culture in an institution of taking Co ownership, of protecting the bank. So we don't create a culture that it's being done by a central team like the CSO only, I think it's really a culture set by senior execs.” (1B)

“To some extent make sure that there is communication and that there's awareness that gets raised in the organization as well and I'm mandating someone to make sure that every employee understands what happens in a

ransomware scenario and what is expected of me as an individual that's the role that senior executives played when we started this journey four years ago with our board and our EXCO." (2C)

4.5 Research objective 4: Investigate how organisations can evaluate the effectiveness of cyber resilience as a mitigating strategy.

Research objective four relates to investigating the various methods and techniques by which organisations can evaluate the effectiveness of cyber-resilience as a strategy to mitigate ransomware attacks.

The findings highlighted the various evaluation methods used to assess the effectiveness of cyber resilience strategies. As the researcher interrogated various methods used for assessing cyber-resiliency, two respondents noted alignment and benchmarking against industry standards as a viable method that can be used for assessing cyber-resiliency in an organisation. The NIST framework was called out as a feasible framework to benchmark against as it covers the critical components of cyber-resilience. ISO standards were also highlighted to provide good guidance when it comes to building cyber-resiliency. Five of the respondents further highlighted the use of red teaming exercises and penetration tests as viable methods to evaluate and assess the cyber-resiliency of an organisation. Respondent 1B highlighted that an organisation can have a checklist in place of elements required for cyber-resiliency, however, without evaluating it through a method such as penetration testing, all that work may be futile. Respondents also suggested that penetration testing could give incident responders an indication of areas they may need to focus on.

"I think another thing too that we use a lot within our institution is obviously this the things that we've just done now the red team exercise because really the proof is in the pudding, is in eating it. You know, that's where we stack it up and say let's look at a real-life scenario where someone is to come in. So we don't just fall into the trap of compliancy. I've got MFA implies tick. I've got antivirus in place. But how well does it stack up to a real-life attack, you know? How will it make it difficult because we all know that with an enough motivation, they will

get in. So it's not that, but it's more of how difficult it is to get in and also how quickly we detect them so that we can contain the damage they do. What the residual risk looks like is by simulating attacks and in giving yourself a view of how well your strategy is stacking up." (1B)

"Then I guess red teaming type exercises, so get people to attack you and you defend against it and try and stop them from deploying ransomware and if they sort of get through and they are able to deploy ransomware, defend against it. So it's testing. That's pretty much the only way making sure you've got coverage." (2C)

Six of the respondents agreed that there is value in employing tabletop exercises and simulations as an assessment method. Tabletop exercises and simulations assist in determining whether the organisation would be able to be resilient against those scenarios if they were to materialise, giving the various role players a level of practice and awareness of how to respond.

"So I think the biggest way is you just you can't just write a strategy and then you put it down and then you don't know if it works or if it doesn't work. So, what you do is you need to test it. You need to do simulation. So you'll do a crisis simulation or you'll do around somewhere tech simulation where you get someone to try and send out this phishing simulations where you try to make to test your users, to see if they're going to click on links and then if they do click on the link, you do remedial training to say, guys, you clicked on this you are not supposed to click on it." (4G)

"Tabletop exercises are encouraged to test people in how prepared they are in a case of an attack" (5H)

Backup, DR, and restoration testing was subsequently also noted as a viable assessment method for cyber resilience in an organisation by four of the respondents. They encouraged that disaster recovery testing should take place for at least 6 to 12 months and have teams test those critical systems, including

payment systems, are able to restore well when the system does come back online.

Two respondents highlighted their views in terms of the use of metrics as an assessment method for cyber resilience:

> “KPI and KRIs. Let me explain something. You know that types of KPI and KRIs. You've got a lagging and a leading KRIs, it normally focuses on things that happened. Things like do you have an incident? How many times this? How many times this type of incident happens, you know? And all those are lagging KRIs. Then you've got leading ones, you know that can enable you to see what you can improve, you know you will be patching but your patching is not that effective. We still have other systems that are out there that are vulnerable and then you can help us to deal with that. So, we need to be careful when we're building KRIs and KPIs because they will tell you your position as an organization.” (1A)

> “They will have to be some sort of metrics and measures that are put in place to actually measure that effectiveness and the success of the remediation plans that we do have. We will have to have some sort of an indicator to suggest and predict where there's a problem and where we are actually doing well. But I also think that it needs to be a robust process. So it's not something that would remain static because ransomware risk is so ever evolving and the complexity of it is something that continuously changes. We obviously need to keep a dial on and our finger on the pulse when it comes to how those threat vectors are actually changing and we will need to have some sort of a way in which we can identify how we need to adapt to those changes and how our business needs to adapt to those changes.” (J1)

4.6 Summary of findings

This chapter presented findings encapsulating the various elements considered in having an effective cyber-resilience strategy for mitigating ransomware cyber-

attacks within South African banks. The researcher presented findings that were collected through semi-structured interviews.

The findings from the study were presented according to the thematic findings identified during the analysis process discussed in Chapter 3, in line with the research objective and research questions. The summary of the findings is encapsulated in the table below, highting the emerging themes and their link to the theoretical model.

Research Objectives	Research Questions	Propositions	Emerging Themes	Theoretical Model
Assess the level of concern and prioritization that organisations have on ransomware cyber-attacks;	Does financial institutions' cybersecurity strategy prioritize the threat of ransomware?	Ransomware is prioritised as a top risk as threat actors' motivation is heightened to exploit financial institutions	1. Ransomware as a top risk 2. Factors driving ransomware to be rated as a top risk 3. Other risks that contribute to the rise of ransomware as a top risk	Threat because ransomware is considered a motivator to the offender
Investigate the key influences that contribute to a cyber-resilient posture of an organisation against ransomware attacks;	What are the factors that influence the cyber resiliency posture of a South African financial institution?	Components derived from the NIST framework (Identify, Protect, Detect, Respond and Recover) are key factors that influence cyber resiliency in financial organisations	1. Awareness of assets and the threat landscape (Situational Awareness/Identify) 2. Ability to protect 3. Ability to Detect 4. Ability to respond and recover	Contributing factor of CR

Assess the role and influence of senior management in influencing the resilient posture against ransomware related cyber-attacks;	How can management’s involvement in establishing a cybersecurity strategy accelerate the organisations’ cyber resilience maturity?	Senior management have a critical role in ensuring cyber resiliency in financial institutions	1. The importance of leadership having a good understanding of the threat landscape 2. Leadership's awareness and understanding of their roles and responsibilities in Cyber resilience 3. Integration of Cyber resilience with business 4. Management prioritising cyber resilience	Contributing factor of CR

Investigate how organisations can evaluate the effectiveness of cyber resilience as a mitigating strategy;	How can financial institutions assess how well their cyber resilience works as a mitigation strategy?	Various methods and techniques can be employed to evaluate the cyber-resilience of an organisation	1. Applying a holistic approach to CR - Integrating Cyber resilience with other strategies, i.e. Defence in Depth for optimal results (C-RAF: Situational Awareness) 2. Benchmarking against industry standards (C-RAF: Governance) 3. Active testing - Red Teaming Exercises, Penetration Tests, Tabletop and Simulation Exercises, Backup, DR, and Restoration Testing (C-RAF: NIST's IPDRR) and iCAST) 4. Use of Metrics (C-RAF: Governance)	Testing CR (use of CRAF)

The next chapter will focus on the discussion of the findings extracted from the semi-structured interviews, linking key points to answering the research question and further supporting a better understanding of the overall research study.

5 Discussion of findings

5.1 Introduction

This chapter discusses and analyses the findings presented in Chapter 4. The aim of the study is to investigate the effectiveness of cyber-resilience as a strategy for mitigating ransomware cyber-attacks within South African banks. Using the research questions to anchor the analysis, the researcher interrogates the level of concern and prioritisation that organisations have for ransomware cyber-attacks and assesses the key factors that contribute to cyber-resilience, including the role that senior management plays in ensuring cyber-resilience in their respective organisations. Finally, the researcher investigates the methods that organisations use to evaluate the effectiveness of a cyber-resilience strategy. The constructs outlined in the conceptual framework in Chapter 2 serve as a key guide in the analysis, taking into consideration the NIST framework's five key components (identify, protect, detect, respond, and recover) as key drivers in ensuring cyber-resilience is regarded as a capable guardian for SA banks against the threat of ransomware.

5.2 Discussion on assessing the level of concern and prioritization that organisations have on ransomware cyber-attacks.

Understanding the level of a risk and how its priority is viewed by the organisation is key to establishing the relevant response strategy for the potential cyber threat. Literature indicates that the cyber threat landscape is evolving, with cyber-attacks on the rise as threat actors develop new techniques for attack paths, using new tools, and establishing new targets to exploit vulnerabilities (Deloitte, 2014).

Ransomware, commonly understood as malware that locks down a file on a victim's computer or device and thereafter demands a ransom from the victim in order for the victim to recover access to the compromised system (Kiru & Jantan, 2019), is one such attack path that continues to wreak havoc in the online world. Financial institutions are not immune to the evolution of attacks, as Petrosyan (2022) demonstrates an increase from 856 reported incidents in 2013 to 2527 in

2021. Moreover, data indicates that attacks are no longer deployed just for financial gains but are focused on destroying data, files, or interrupting services or networks (Gulyás & Kiss, 2023). Supporting this, according to Doerr et al. (2022), financial institutions host substantial amounts of data where customers rely on them to maintain data confidentiality as well as integrity; additionally, the availability of service is of paramount importance to service customers, which makes financial institutions attractive targets for attackers. In line with this, the findings outlined in Chapter 4 support this notion, as it emerged that while SA banks have a number of assets to protect, they also need to ensure the CIA of the bank is maintained; otherwise, the repercussions, including customer, financial, and even regulatory impacts, can be dire to any of the banks. This level of potential impact makes it attractive to likely offenders, and in respects to a suitable target, this makes SA banks attractive targets, who without a capable guardian of their crown jewels can suffer exceptional impact.

The introduction of services such as ransomware-as-a-service (Raas) is also highlighted as a concern. RaaS is described as a business model where ransomware is sold or even rented to buyers, who can then deploy it to organisations and demand ransomware (Kibet et al., 2022). Respondents cite this as a concern, as the ease of deploying ransomware from RaaS inherently increases the likelihood of multiple attacks or attempts thereof as threat actors no longer require the technical skills to deploy such an attack.

The risk of third-party and insider threats was also highlighted as something organisations need to concern themselves with when it comes to ransomware. It is noted that threat actors target third-party organisations that may have low cyber-resiliency, and once they have successfully compromised their network, they are able to attempt access into other organisations that could include SA banks. Groves & Garcia (2021) support the idea that ransomware on third-party providers has an elevated risk of a large blast radius and has an exceptional impact compared to if only one organisation is targeted. This remains a substantial risk as many organisations integrate their systems, making it easier to gain access to multiple other networks once the main supplier is compromised.

On an insider threat, Khan et al. (2023) discusses that insider threats at times may be unintentional but still pose a significant risk to the organisation. A staff member may unintentionally click on a phishing link, compromising the network

or sharing sensitive information, allowing threat actors to launch an attack. One cannot, however, ignore the likelihood of an intentional insider threat; the Cybersecurity and Infrastructure Security Agency (2023) references this kind of insider threat as a “malicious insider”. This type of threat actor leverages their internal elevated access in an organisation to deliberately disrupt services, steal data, identify weaknesses in the IT systems, and collude with other threat actors to launch an attack.

Overall, with respect to ransomware being considered a top risk, it emerged that ransomware is considered and rated a top risk by all the SA banks, with board-level visibility and various cybersecurity programmes put in place to remediate all potential gaps and vulnerabilities.

5.2.1 Discussion on the investigation of the key influences that contribute to a cyber-resilient posture of an organisation against ransomware attacks.

According to the definition by DuPont (2019), it is understood that cyber-resilience is “the capacity to withstand, recover from, and adapt to the external shocks caused by cyber risks.” Complementing this understanding of cyber-resilience, the researcher takes guidance from the five key components of the NIST framework and posits them as key influences that contribute to cyber-resiliency in an organisation, as discussed in chapters 1 and 2. Additionally, Conklin et al. (2017) share seven generic principles, which are described as the “Cyber Resilience Process”, where the principles described are closely aligned and comparable to the various steps outlined in the NIST framework. The findings outlined in Chapter 4 support this notion of the NIST framework's five components (identify, protect, detect, respond, and recover) as the ideal basis of key constructs for ensuring cyber-resiliency. Furthermore, this is in line with the conceptual framework discussed in Chapter 2, where the NIST components are deemed to be contributing factors to cyber-resilience.

5.2.2 The ability to identify.

Cyber resilience requires a good understanding of what 'success' looks like to equip organisations with a satisfactory level of preparedness when facing cyber-

attacks. One of the core functions within the NIST framework is to be able to adequately identify key elements in any business, which may include company assets, critical information, or systems, as well as capabilities that the organisation critically depends on to ensure business continuity (NIST, 2018). In the bid to understand the success factors that contribute to cyber-resiliency, awareness of one's assets emerged from the findings, aligning well with best practices and guidelines provided by the NIST framework. One respondent posits, “You cannot protect what you do not know,” which is a factor that contributes to determining whether a resilience strategy makes sense for the said organisation. The “classify” principle presented by Conklin et al. (2017) supports this by putting emphasis on the fact that you cannot protect assets you do not know exist.

It is also key to note from the findings that this is not limited to the awareness and understanding of the internal environment but also the external environment. As the threat landscape evolves, the internal controls need to be adjusted accordingly to provide consistent prevention and protection.

5.2.3 Ability to protect.

In considering the threat landscape, one of the key factors that organisations venture into to ensure that there is adequate resilience from potential cyber threats is to ensure that the organisation can effectively protect itself. Protection may come in various forms to ensure the comprehensive safeguarding of critical infrastructure. The guidance provided by NIST (2018) includes the protection categories of identity management and access control; awareness and training; data security; information protection processes and procedures; maintenance; and protective technology. In support of this, the findings outlined in Chapter 4 demonstrate various aspects of how organisations can ensure that there is adequate protection at all levels. This includes ensuring that there is organisational awareness of the threat of ransomware, inclusive of staff that may not be directly working in an IT or cybersecurity role, as humans are deemed a critical part of the protection element as it takes one person clicking on a malicious link to potentially infect a network. According to Triplett (2022), the human element should remain at the centre of any business operations, and more

so in building cyber resilience. Supporting the human element aspect of protection, the findings encourage training and awareness among all staff members. Additional protection mechanisms highlighted include hardening an environment in line with best practices, having secure configuration on firewalls, consistently applying patches, safeguarding systems, services, and admin accounts, disabling removable media ports, etc. While there may be many other ways to ensure protection, the findings are aligned in that organisations need to invest in ensuring their environment is adequately protected as part of building their cyber-resiliency.

5.2.3 Ability to Detect

Taking guidance once again from the NIST framework, it is of importance to understand the criticality of the 'Detect' function when formulating a cyber-resilient strategy. The detect function plays a vital role in ensuring that, in the event of an attack, the organisation can promptly detect and respond accordingly to minimise the level of impact that the attack may have on the organisation (NIST, 2018). While literature shows that detection techniques are maturing (Kapoor et al., 2021), it emerged in the findings that there are instances where organisations are not aware that a cyber-incident has even occurred until a few weeks later or organisational data is uncovered in the dark web. This brings the detection function under the spotlight, as in the case of a ransomware attack, organisations need to be alerted as soon as possible so that they can respond swiftly to limit the level of impact.

5.2.4 Ability to respond and recover.

The ability to respond and recover emerged as a prevalent factor that contributes to cyber-resilience. Lending from the discussion highlighted in Chapter 2, Pearlson et al. (2021) posit that "it is not about if an attack will happen, but rather when it will happen". This puts a responsibility on organisations to ensure that when an attack does happen, they are able to promptly respond to reduce the blast radius as well as recover as quickly as possible to minimise the impact on business operations. Findings support this notion, indicating that a lot of the focus in their cyber-resilience strategy is placed on the response and recovery aspect, as they anticipate that a ransomware attack will eventually take place in their

respective organisations and thus need to be adequately prepared for the eventuality. A large component of recovery includes ensuring immutable and offline backups, as this was identified as the one area that threat actors leverage when demanding ransom. This vector includes targeting backups and encrypting them, knowing that the organisation will be at their mercy to resume business activities, and may also indicate a loss in confidentiality and integrity (Aurangzeb et al., 2017).

5.3 Role of Senior Management

As noted in the literature review, ransomware as a cyber-threat has gained heightened focus at the various leadership levels, all the way to the board of South African banks (Tuttle, 2021). Sitting at the helm of big corporate organisations, senior management is encouraged to be well versed in the cyber threat landscape and understand their business well so that they can adequately support efforts to prevent and mitigate any cyber-related threats. Findings from chapter 4 on assessing the role and influence of senior management on cyber-resilience support the notion that senior management ought to have a good understanding of the risks and threat landscape that will influence their decision-making and support for cybersecurity initiatives. Furthermore, an emerging theme is overall accountability. One of the prominent discussions that emerged in the literature review is that of accountability for the overall cybersecurity of the organisation. This is noted as an aspect that needs to be clearly articulated and understood across the business of who from the senior leadership will be accountable for leading and responding to cybersecurity and ultimately the resilience of the organisation, with literature proposing that the CISO take on the overall accountability (Reilly et al., 2016). In Chapter 4, however, the findings contrast this and encourage shared accountability by senior management across the organisation. This stance is supported by the notion that ensuring cyber-resilience is not separate from the rest of the business and should, in fact, form part of the business strategy. Business operations are often intertwined with an organisation’s network infrastructure, where lateral movements can be deployed. It is therefore important that each business unit is invested in ensuring cyber-

resilience. In line with the conceptual framework, senior management is noted as a key contributor to enabling cyber-resilience in an organisation.

*5.3.1 **Prioritizing Cyber-resilience***

A further emerging theme outlined in Chapter 4 is for senior management to ensure that cybersecurity and building cyber resilience are prioritised at the various levels, from the board to the business. Supporting this view, Bajpai & Enbody (2020) firmly position that ransomware has been a top threat and concern, which is looked at by senior management. Linked to the accountability of cyber-resilience spanning across businesses, some of the views include ensuring that cyber-resilience is flagged as a business risk rather than an IT or CSO risk. Prioritising cyber-resilience includes ensuring that the cybersecurity teams are adequately resourced, with continuous upskilling to keep up with the changing threat landscape. Al-Alawi et al. (2019) support this by positioning that senior management needs to place cybersecurity as a top priority, and this should reflect in the budget allocations to ensure that the organisation is armed with sufficient resources and security controls to promise adequate cyber-resiliency.
Additionally, findings also indicate that if the whole organisation prioritises cyber-resilience, it will receive sufficient airtime in senior management and even board-level meetings and discussions, where key decisions can be taken with regards to issues around budgeting, rolling out specific programmes, assessment of the strategy (Bagheri et al., 2023). One other way that was noted in the findings for senior management to prioritise ransomware across the business is through the participation of simulations. Senior management across the business spending time to participate in attack simulations helps them be better prepared for when an attack does take place. The highlighted risk is shifted from just theory documented in risk packs to potentially practical examples where management needs to practice their responses, which may also support awareness of risk criticality and help to increase focus amongst senior leaders.

5.3.2 Encouraging a cyber-resilient culture

Linked to the integration with business leaders and business strategy, one of the key roles that senior management is noted to do is to drive a culture that

encourages cyber-resilience across the organisation, as well as ensuring that the respective teams are well resourced and skilled to adequately mitigate cyber threats. In the event of an attack, they are expected to be able to respond adequately and effectively to reduce the impact of the attack. Literature in Chapter 2 supports the notion that senior management needs to promote the training and education of cybersecurity across the organisation, as this helps to increase human defences and subsequently resilience against cyber threats (Triplett, 2022). Findings also indicate that culture enables the staff to know how to respond in a case of an attack, where if staff members are aware of the risks of clicking links leading to potential ransomware attacks, they would function as a layer of defence by reporting any suspicious links.

5.3.3 Discussion on the evaluation of cyber-resilience

In the rapidly changing digital environment and cyber threat landscape, the assessment techniques used to determine the effectiveness of cyber-resilience have assumed increasing importance. The literature outlined in Chapter 2 suggests that for organisations to assess the effectiveness of cyber-resilience measures to ensure that they have the capacity to withstand and recover from cyber-attacks, various methods and techniques must be considered (Bodeau et al., 2018). While there are several evaluation methods available, the researcher takes note of the Cyber Resilience Assessment Framework (C-RAF) as a framework viable to marry with the NIST framework when assessing cyber-resilience, noting similarities in the components both frameworks focus on with respect to ensuring cyber-resiliency, i.e., identification, protection, detection, response, and recovery (Deloitte, 2023). The findings in Chapter 4 discuss various methods that organisations can employ to assess the effectiveness of the cyber-resilience discussed below. With respect to the conceptual framework referenced in Chapter 2, the assessment of cyber-resilience provides validation of the effectiveness of cyber-resilience as a present capable guardian.

5.3.4 Benchmarking against industry standards

An emerging theme from the findings includes consideration of cybersecurity standards that provide the industry with a number of guidelines and best

practices. Organisations can adapt and apply these guidelines, respectively, to ensure that they have adequate protection against cyber-attacks and, in the event of a successful cyber-attack, would be able to adequately respond and recover. Supporting this, Taherdoost (2022) highlights that a framework does not prescribe for an organisation to adopt specific options but rather acts as a guidance note for organisations. Findings identified the NIST framework as well as ISO standards as common frameworks and standards that organisations can use to benchmark their level of cyber-resilience. This is also in line with and supported by literature, as covered in Chapter 2.

5.3.5 Red Teaming Exercises and Penetration Tests

An agreement emerged from the findings of red teaming exercises and penetration tests highlighted as viable methods of assessing cyber resilience. According to the findings, red teaming exercises and penetration tests both emerged as prominent security assessment methods used to determine flaws and vulnerabilities in an organisation's systems, processes, and/or infrastructure. These assessment methods share similarities, but there are distinct differences in their approach and scope.

Mansfield-Devine (2021) discusses the main differences between a red team exercise and a penetration test by citing that getting skilled hackers in to test and reveal any system or technical vulnerabilities or weaknesses is the main idea behind penetration testing, while one would engage in a red teaming exercise to look for more objective-led vulnerabilities. In an example to demonstrate the differences, Mansfield-Devine (2021) highlights a red teaming exercise as one that would be focused on answering the question "How could I use this application to get hold of a piece of valuable data—a critical customer database, for instance", This would include instances of social engineering and not necessarily be limited to technical vulnerabilities. Whereas for a penetration test, one would focus on the technical vulnerabilities specific to systems, applications, or networks. Findings in Chapter 4 point to red teaming exercises and penetration tests being the ultimate tests of whether the cyber-resiliency strategy is working effectively or not. In the Intelligence-led Cyber-Attack Simulation Testing (iCAST) discussed in Chapter 2, red teaming exercises and penetration testing are also

highlighted as key activities in assessing the effectiveness of cyber-resilience. Under iCAST, penetration testing includes threat information and additional knowledge verification of the penetration tester(s) to the typical penetration test to create end-to-end testing scenarios, allowing for simulations close to real-life attacks.

5.3.6 Tabletop and Simulation Exercises

According to Brilingaitė et al. (2017), the key objectives of a tabletop exercise are to imitate real-life cyber incidents and the roles that various stakeholders would assume in investigating and managing a cyber incident. Tabletop exercises are often paper-based, presenting various scenarios where different parties can test their involvement, processes to be followed, and decisions that need to be made at the various stages of an incident, all-inclusive of managing even regulatory-related responses that may be required in a case of an attack. By nature of design, findings in Chapter 4 identify tabletop exercises as a viable assessment method of cyber-resiliency at a senior management and even board level, with suggestions that simulation exercises provide a view of how well the cyber-resilience strategy is stacking up.

5.3.7 Backup, DR, and Restoration Testing

Many organisations heavily rely on data and technology systems to conduct their daily business and internal operations, which inherently puts many organisations at risk for system failures or even data loss in the event of a cyber-attack (Kekwaletswe & Modiba, 2020). Findings highlight that to ensure that organisations can maintain the CIA as well as the business continuity of their business, they need to ensure that, in the event of a successful attack, they will be able to swiftly recover. It emerged in the findings that having backups, a disaster recovery plan, and a business continuity plan in place may be a good strategy for cyber-resiliency; however, it is also good practice for organisations to regularly test to ensure that in the event of a real attack, the organisation will have the best chance of quick recovery. Bodeau et al. (2018) support this, encouraging the assessment of the effectiveness of the employed cyber-resilience strategy to ensure that they are adequately prepared in case of an attack. Findings indicate

that additional testing of backups, disaster recovery, and restoration is also a viable method to assess whether the employed component of recovery is operating in an effective manner.

5.3.8 Use of Metrics

Metrics and measures are well-known mechanisms employed across various industries and organisations to measure how well they are performing at a particular activity. Bodeau et al. (2018) highlights that metrics provide organisations with the ability to identify, describe, and track how well implemented controls, efforts, and performances enable the achievement of cyber-resilience objectives. It is therefore no surprise that metrics are highlighted as an assessment method for cyber-resilience in the findings in Chapter 4. Metrics are positioned to provide critical insights on external cyber-threat trends, assessments of internal vulnerabilities and security gaps, as well as leading indicators for the probability of recovering from an actualized cyber-attack. Findings suggest that both lagging and leading indicators need to be employed for more accurate measurement and can provide a holistic assessment of whether the employed cyber-resilience strategy is indeed effective.

5.4 Conclusion

In this chapter, the findings outlined in Chapter 4 were discussed in line with the research objectives posed in Chapter 1. The chapter provides an overview of the discussions highlighted in the literature review, contrasting ideas, themes, and topics with the findings outlined in Chapter 4, which were derived from the semi-structured interviews conducted as part of the study. Additionally, various frameworks, including the conceptual framework presented in Chapter 2, is used to link the data collected with the concepts discussed in Chapters 1 and 2. The next chapter will focus on the conclusion of the study, testing the propositions put forward in Chapter 2, as well as positioning recommendations to be considered as a result of this study.

6 Conclusions and Recommendations

6.1 Introduction

This chapter draws the conclusion of the research study as well as provides the overall recommendations and suggestions for future studies. The conclusion and recommendations are based on the literature reviewed on the topic as discussed in Chapter 2 and the data collected as outlined in Chapter 4 and discussed in Chapter 5.

This study investigated the extent and effectiveness of employing a cyber-resilience strategy in mitigating ransomware cyber-attacks. Additionally, the study explores frameworks and factors that contribute to ensuring that a cyber-resilience strategy is effective and can withhold the ever-changing cyber-threat landscape.

It emerged in the literature that many organisations, including financial institutions, are embracing digital transformation in order to maintain their market positioning within a competitive market; consequently, this introduces an inherent risk of increased cyber-attacks, where cyber incidents are noted to be on the rise, with COVID-19 evidently causing a surge in cyber-attacks on financial institutions. Additionally, as the cyber-threat landscape evolves, ransomware emerges as a growing threat, as it is attractive to threat actors who can demand ransom from organisations, they are able to penetrate and deploy malware.

Literature further highlights the focus areas of a cyber-resilience strategy and how the principles underpinning strategy can be linked to the NIST framework, which provides organisations with effective guidance on ensuring they can prevent, withstand, or even recover from a cyber-incident.

The research questions, in alignment with the problem statement, propositions, and purpose of the study, are used to formulate appropriate conclusions and recommendations.

6.2 Conclusion regarding RQ1.

The rapid evolution of the cyber-threat landscape remains a concern for all organisations and industries alike. Consequently, ransomware remains a top priority for organisations; in this context, SA banks are noted to be suitable targets

because of the nature of their business. Threat actors are motivated by the possible monetary value and even power they may get if they can successfully infiltrate a bank. It is of particular concern that threat actors no longer have to rely on high technical skills to launch such attacks and can leverage things like RaaS and even artificial intelligence. Considering all this, SA banks should continue to prioritise ransomware as a top risk.

6.3 Conclusion regarding RQ2.

The NIST framework provides good foundational guidance in identifying areas of focus for building cyber-resilience. With five key components, including identify, protect, detect, respond, and recover, employing the strategy with these as a guide provides a sense of multiple levels of defence and mitigation against a possible cyber-attack. However, it is key to note that both literature and findings highlight that the probability of a ransomware attack remains exceptional; thus, the response and recovery components are a focal point when designing cyber-resiliency to ensure that there is the least impact in the case of a successful attack. This does not nullify the other components to identify, protect, or detect, as these too play a critical role as a defence mechanism.

6.4 Conclusion regarding RQ3.

Effective leadership in an organisation remains critical to ensuring the success of the organisation. This is true even when it comes to building a cyber-resilience strategy for the organisation. To ensure the success and effectiveness of employing a cyber-resilience strategy, senior management needs to be aware of the risks associated with ransomware attacks on their business. To accomplish this, there needs to be shared accountability across business leaders, ensuring that cyber-resiliency is prioritised and incorporated into the business strategy rather than seen as an isolated and independent task. The rest of the organisation also looks to senior management to set the tone and, thus, the culture of items to be concerned about. To promote a cyber-resilience culture, senior management thus needs to invest in the education and training of all staff members on matters of cyber-resilience and ensure that there are adequate skilled resources and heightened visibility and discussions at various forums.

6.5 Conclusion regarding RQ4.

Establishing a cyber-resilient strategy is beneficial to any organisation; however, one must not miss the importance of assessing the effectiveness of the strategy for the specific organisation. Each organisation is at liberty to choose which evaluation methods to employ as part of the assessment; conversely, this study establishes that frameworks such as the Cyber Resilience Assessment Framework (C-RAF) are viable for organisations to use to assess the effectiveness of their cyber-resilience strategy, as they are well aligned with the components outlined in the NIST framework. These are noted to be foundational constructs of a cyber-resiliency strategy.

6.6 Recommendations

Considering the results of the findings, analysis, and discussions outlined leading to the conclusions, below are recommendations on what SA banks can consider when employing cyber-resilience as a strategy to prevent and mitigate ransomware attacks:

1. Organisations should keep ransomware a top priority, employing different techniques to ensure rapid detection and response because of an evolving threat landscape and the introduction and use of technologies such as artificial intelligence, which could catch many organisations off-guard if not well prepared.

2. Incorporating cyber-resilience as part of an overall cybersecurity strategy will ensure that the various components of building cyber-resiliency are prioritised across the organisation on all levels.

3. Senior management to collectively lead the cyber-resilience narrative in the organisation, embedding it as part of the overall business strategy and encouraging a cyber-resilient culture in the organisation.

4. Aligning cyber-resiliency practices with industry best practices and frameworks, such as the NIST framework, as a benchmark

5. Design and engage in regular testing and assessment of the strategy to evaluate its effectiveness and identify areas where improvement may be required.

6. Refrain from using only one strategy when it comes to mitigating cyber-attacks. While cyber-resilience is noted to be an effective strategy, marrying other strategies, such as defence, in depth will increase the effectiveness of preventing and mitigating ransomware attacks.

6.7 Suggestions for further research

This research study provided insights on the use of cyber-resilience as a strategy for mitigating ransomware cyber-attacks in the context of SA banks. Literature and findings indicate that cyber-attacks continue to grow, with ransomware becoming a popular attack vector used by threat actors. The study notes there are factors that contribute to the effective cyber-resilience of an organisation, and as such, additional research delving into these specific factors should be considered for future research. The role of leadership in building cyber-resiliency is one such area of research that is recommended to be further explored, as this is noted to be an important aspect of building effective cyber-resiliency. Additionally, people are highlighted as a key cyber-defence component, and topics around adequately empowering the human factor as a defence are recommended to be explored. Incidents involving ransomware and the level of cyber-resilience that organisations have are not widely covered, more so in a South African context. Further research in understanding the true frequency, impact, and even likelihood of ransomware attacks in SA banks will be beneficial in enabling the industry to build even more effective cyber-resiliency within their organisations. Additionally, research worth further exploring is on the role that risk management practices play in managing cyber-attacks.

7 REFERENCES

Akinbowale, O. E., Klingelhofer, H. E., & Zerihun, M. F. (2023). The assessment of the impact of cyberfraud in the South African banking industry. Journal of Financial Crime, 1-15.

Al-Alawi, A. I., & Al-Bassam, S. A. (2019). Assessing the factors of cybersecurity. Arab Gulf Journal of Scientific Research, 37(4), 17-32.

Asmundson, I. (2011). What are financial services. Finance & Development, 48(1), 46-47.

Aurangzeb, S., Aleem, M., Iqbal, M. A., & Islam, M. A. (2017). Ransomware: A survey and trends. Journal of Information Assurance and Security, 12(1), 1-11.

Bagheri, S., Ridley, G., & Williams, B. (2023). Organisational cyber resilience Management perspectives. Australasian Journal of Information Systems, 27, 1-28.

Bajpai, P., & Enbody, R. (2020). Preparing smart cities for ransomware attacks. In Proceedings of the 2020 3rd International Conference on Data Intelligence and Security (pp. 127-133). South Padre Island, TX, USA.

BasuMallick, C. (2022, May 20). What is botnet? Definition, methods, attack examples, and prevention best practices for 2022. Spiceworks.

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges, and future research directions. Elsevier, 111, 1-22.

Bearman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021, December). Ransomware: Recent advances, analysis, challenges, and future research directions. Computers & Security, 111.

Bhatia, M. K. (2017). Data analysis and its importance. International Research Journal of Advanced Engineering and Science, 2(1), 166-168.

Blafka, B. (2023, March 24). History of digital transformation.

Bodeau, D. J., Graubart, R. D., McQuaid, M. R., & Woodhill, J. (2018). Cyber resiliency metrics, measures. Bedford, MA: The MITRE Corporation.

Bodeau, D. J., Graubart, R. D., McQuaid, R. M., & Woodhill, J. (2018). Cyber resiliency metrics catalog. Bedford, MA: The MITRE Corporation.

Brewer, R. (2016, September). Ransomware attacks: Detection, prevention, and cure. ScienceDirect, 2016(9), 5-9.

Carnegie. (2023). Carnegie: Endowment for international peace. Retrieved from https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline

Carter, S., & Henderson, L. (2005). Approaches to qualitative data collection in social science. In A. Bowling & S. Ebrahim (Eds.), Handbook of health research methods: Investigation, measurement, and analysis (pp. 215-230). McGraw-Hill Education.

Carter, W. A., & Crumpler, W. D. (2019). Financial sector cybersecurity requirements in the Asia-Pacific region. Center for Strategic & International Studies.

Conklin, W. A., Shoemaker, D., & Kohnke, A. (2017). Cyber resilience: Rethinking cybersecurity strategy to build a cyber resilient architecture. In T. Mokoteli (Ed.), Proceedings of the 12th International Conference on Cyber warfare and Security (pp. 105-111). Academic Conferences and Publishing International Limited.

Crowdstrike. (2017, June 17). WHAT IS A TROJAN HORSE? Retrieved May 26, 2023, from https://www.crowdstrike.com/cybersecurity-101/malware/trojans/

DefenceWeb. (2023, April 06). South Africa in top five countries affected by cybercrime in 2022. Retrieved May 06, 2023, from https://www.defenceweb.co.za/cyber-defence/south-africa-in-top-five-countries-affected-by-cybercrime-in-2022/

Deloitte. (2014). Transforming cybersecurity: New approaches for an evolving. Deloitte Centre for Financial Services.

Deloitte. (2023). Cyber Resilience Assessment Framework (C-RAF) 2.0. Retrieved from https://www2.deloitte.com/cn/en/pages/risk/articles/cyber-resilience-assessment-framework.html

Doerr, S., Gambacorta, L., Leach, T., Legros, B., & Whyte, D. (2022). Cyber risk in central. Bank for International Settlements.

Group IB. (2018). The evolution of ransomware and its distribution methods.

Guion, L. A. (2002). Triangulation: Establishing the validity of qualitative studies. University of Florida.

Gulyás, O., & Kiss, G. (2023). Impact of cyber-attacks on the financial institutions. Procedia Computer Science, 219, 84-90.

Gura, D. (2023, March 10). A Silicon Valley lender collapsed after a run on the bank. Here's what to know. NPR. Retrieved from https://www.npr.org/2023/03/10/1162599556/silicon-valley-bank-collapse-failure-fdic-regulators-run-on-bank

Hong Kong Monetary Authority. (2016). Cyber resilience assessment framework. Retrieved from https://uploads-ssl.webflow.com/59d28ad983887e000196f803/5fecc1fe13498132b4fa835b_HKMA%20CFI%20-%20Cyber%20Resilience%20Assessment%20Framework%20-%20Dec%202016.pdf

Imeson, M. (2020, September 02). Ransomware threat tests banks' resilience to cyber-crime. TheBanker. Retrieved from https://www.thebanker.com/Transactions-Technology/Ransomware-threat-tests-banks-resilience-to-cyber-crime

IT Governance. (2022). What is COBIT 5.

Johnson, G., Whittington, R., Regner, P., Scholes, K., & Angwin, D. (2011). Exploring strategy: Text and cases (11th ed.). Pearson.

Kansagra, D., Kumhar, M., & Jha, D. (2015). Ransomware: A threat to cybersecurity. International Journal of Computer Science and Communication, 7(1), 224-227.

Kiru, M. U., & Jantan, A. (2019). The age of ransomware and its countermeasures. In M. U. Kiru & A. Jantan (Eds.), Artificial intelligence and security challenges in emerging networks (pp. 1-37).

Lee, H. (2016, May 18). Cybersecurity summit 2016: The cyber resilience assessment framework. Retrieved from https://www.hkma.gov.hk/media/eng/doc/key-information/speeches/s20160518e2.pdf

Leventopoulos, S. A. (2022). Retaliation within the scope of cybersecurity. Athens University of Economics and Business.

MARSH. (2023). Ransomware stats every business needs to know.

McCain, N. (2023, May 23). Going dark: Cyber-attack on Western Cape parliament downs ICT systems. News24. Retrieved from https://www.news24.com/news24/southafrica/news/going-dark-cyber-attack-on-western-cape-parliament-downs-ict-systems-20230523

Mohajan, H. K. (2018). Qualitative research methodology in social sciences and related subjects. Journal of Economic Development, Environment and People, 7(1), 23-48.

Nabe, C. (2023). Impact of COVID-19 on cybersecurity. Retrieved from https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html

National Cyber Security Centre. (2023). Measuring resilience. Government Communications Security Bureau. Retrieved from https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Charting-Your-Course-Governance-Step-6-Nov-2019.pdf

Ngila, F. (2022, September 08). South Africa’s banking and insurance sectors are overwhelmed by cyber-attacks. Retrieved from https://qz.com/south-africa-is-overwhelmed-by-hackers-1849510056

NIST 800-53A. (2022). Assessing security and privacy controls in. National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar5.pdf

NIST. (2014). Framework for improving. National Institute of Standards and Technology. Retrieved from https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf

NIST. (2023, July 06). NIST risk management framework RMF. Retrieved from https://csrc.nist.gov/Projects/risk-management/about-rmf/select-step

Ogunjuyigbe, O. (2022, September 12). South Africa's thriving banking sector is vulnerable to cybercrime. Venture. Retrieved from https://venturesafrica.com/south-africas-thriving-banking-sector-is-vulnerable-to-cybercrime/

O'Kane, P., Sezer, S., & Carlin, D. (2018). Evolution of ransomware. IET Networks, 7(5), 321-327.

Patton, M. Q. (1999). Enhancing the quality and credibility of qualitative analysis. HSR: Health Services Research, 34(5), 1189-1208.

Petrosyan, A. (2022, August 31). Cyber-crime & security. Statista. Retrieved from https://www.statista.com/statistics/1310985/number-of-cyber-incidents-in-financial-industry-worldwide/

PWC. (2023). Unlocking growth in complex conditions: South Africa - Major banks analysis. PWC. Retrieved from https://www.pwc.co.za/en/assets/pdf/major-banks-analysis-march-2023.pdf

Reilly, M., Alexander, A., & Cummings, J. (2016). The rise of the chief information security officer. SHRM Executive Network. Retrieved from https://www.shrm.org/executive/resources/people-strategy-journal/winter2016/pages/chief-security-info-officer.aspx

SABRIC. (2023). Digital banking crime statistics. Retrieved from https://www.sabric.co.za/media-and-news/press-releases/digital-banking-crime-statistics/

SARB. (2022). Prudential authority - Assessment of money laundering, terrorist financing and proliferation financing risk in the banking sector. Retrieved from https://www.resbank.co.za/content/dam/sarb/publications/media-releases/2022/pa-assessment-reports/Banking%20Sector%20Risk%20Assessment%20Report.pdf

Skelton, A. (2017). Analyzing cyber threats affecting the financial industry. Retrieved from https://commons.erau.edu/cgi/viewcontent.cgi?article=1062&context=student-works

Skog, D. A., Wimelius, H., & Sandberg, J. (2018). Digital disruption. Business Information Systems Engineering, 60(5), 431-437.

Triplett, W. (2022, July 22). Addressing human factors in cybersecurity leadership. Cybersecurity and Privacy, 2(3), 573–586. Retrieved from https://doi.org/10.3390/jcp2030029

U.S. Department of Homeland Security. (2020). Cyber resilience review (CRR) - Method description and self-assessment user guide. Carnegie Mellon University.

U.S. Department of Homeland Security. (2020). Cyber Resilience Review Fact Sheet. Carnegie Mellon University.

Yates, J., & Leggett, T. (2016). Qualitative research: An introduction. Radiologic Technology, 87(2), 225-231.

APPENDIX A: Information sheet

Dear Sir/Madam

My name is Nqobile Mahlangu, and I am a student at the Wits Business School. I am currently completing research in fulfilment of my master's in management, in the field of Digital Business under the supervision of Dr Kiru Pillay.

To complete my thesis, I am required to conduct interviews to gather data on my topic, which is **'Strategies to mitigate ransomware related cyber-attacks in South African financial institutions.'** The research aims to understand what factors influence cyber resilience for financial institutions, how the involvement of management can assist in accelerating a cyber-resiliency maturity and how the adoption of frameworks, standards and best practices can provide effective guidance when adopting cyber resilience as a strategy for ransomware related attacks.

In that regard, I would like to invite you to take part in my research in a form of an interview. The interview should take no more than an estimated 60 minutes of your time and would be conducted via MsTeams.

By participating in this study, you will not receive any direct benefits such as payment or similar benefits. Please note that there are no disadvantages or penalties for non-participation. You may withdraw your participation from the interview as well as choose not to answer any question that you do not wish to at any time. All responses collected from the interview process will be treated with confidentiality and anonymously, with no identifying information that will be required at any point.

I am available to answer any questions you may have relating to the research, and you are free to contact with me via the details provided below.

A final report on this research will be produced and submitted to the Wits Graduate School of Business. Should you be interested to receive a summary of the report, I will make one available to you.

Please be so kind to accept my invitation - which will come in a separate mail as an MsTeams meeting invite. Attached in this mail is the *ethics certificate* and *participation consent* form for completion to give you comfort that this research will be carried out in an ethical manner.

Should you have concerns or complaints regarding this study's ethical procedures, you are welcome to contact the University Human Research Ethics Committee (Non-Medical), telephone +27(0)11 717 1408, email Shaun.Schoeman@wits.ac.za.

Yours sincerely,

Student: Nqobile Mahlangu

Email: 2159255@students.wits.ac.za

Supervisor: Kiru Pillay

Email: Kiru2010@gmail.com

APPENDIX B: Agreement form

Consent to take part in research.

I……. voluntarily agree to participate in this research study.

I confirm that the information contained in Information Sheet document was explained to me by Nqobile Mahlangu and I have received a copy that I can reference at any point of my participation.

Nqobile gave me the opportunity to ask questions to clarify where I was not clear, and all questions were answered to my satisfaction. I understand that the interviews will be audio recorded unless otherwise I explicitly state otherwise. I hereby consent to participate in this research voluntarily.

I understand that even if I agree to participate now, I can withdraw at any time or refuse to answer any question without any consequences of any kind.

Participant:

Signature:…….
Date:……..

Researcher:

I, Nqobile Mahlangu believe the participant is giving informed consent to participate in this study.

Signature:…….
Date:……..

(Signed consent will be obtained from the respondent prior to the commencement of the interview)

APPENDIX C: Interview guide

Script:

Welcome and thank you for taking the time to participate in my research. My name is Nqobile Mahlangu, I am a student at the University of Witwatersrand studying towards my master's in management in the field of Digital Business. The aim of my research project is to investigate the extent and effectiveness of cyber resilience strategies in mitigating ransomware related cyber-attacks within the South African financial sector. As a Cybersecurity professional, I value your opinions and insights that could contribute towards my study. The interview I have prepared will take approximately 60 minutes to an hour and will include 14 questions where you can share your opinions and insights on themes around cyber-resiliency, the level of management's involvement in activities surrounding ransomware and general cyber-attack mitigating strategies. A gentle reminder that all your responses will remain confidential and are considered as your personal views and not those of your organisation. I would like to request your permission to record the interview for the purposes of accurately documenting the information you convey. If at any time you during the interview you wish to discontinue the recording of the interview or the interview itself, please feel free to let me know. Are you comfortable for me to record? *{Acknowledge permission granted/or not granted}*

Prior to this interview, I shared with you an introductory letter as well as consent forms, one to sign and return to me, and another for you to keep. The consent forms serve as a purpose of certifying that you agree to voluntarily continue with this interview.

At this time, I would like to remind you that your participation in this interview is completely voluntary. You may at any point request that we stop, take a break, or revisit a question.

Do you have any questions or concerns before we begin with the interview?

With your permission, I will now begin the recording of the session and begin the interview.

-------end--------

Interview Questions:

Section 1: Is Ransomware a problem that financial institutions are worried about?

1. Ransomware is commonly understood as a form of malware that is designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors would then demand ransom in exchange for decryption. Would you then say that ransomware attacks are considered a top risk for senior management in your organisation?

2. Considering the current cyber-attack threat landscape, how big of a threat do you think Ransomware attacks are to South African Financial Institutions – specifically banking?

Discussion Point: Cyber resilience is described as the organization's ability to recover data, avoid service disruption, and mitigate overall damages and while ensuring a successfully recover from adverse cyber events.

3. In your view, how cyber resilient would you say is your institution against ransomware attacks?
   Prompt Question: how effective is the adoption of a cyber-resilience strategy in mitigating ransomware related attacks?

Section 2: What mitigation strategies are being considered by Financial Institutions to mitigate ransomware attacks?

4. In your view, what are the key factors or components that contribute to a cyber-resilient posture of an organisation against ransomware attacks?

5. How can institutions evaluate if an adopted cyber-resilient strategy is effective at mitigating Ransomware attacks?

6. How different is your strategy for ransomware as compared to other attack paths?

7. In your view, what needs to be in place to ensure that there is constant and consistent improvement of cybersecurity within organisations to mitigate against the ever-evolving threat landscape?

Section 3: What is the value of top management's involvement in establishing a cybersecurity strategy to accelerate the organisations' cyber resilience maturity?

8. In your view, what role do you think senior management should play in influencing the cyber resilient posture against Ransomware?

9. In your view, what can senior management do to accelerate the organisations' cyber resilience maturity to mitigate against ransomware?

------end------

Script:

We have reached the end of our interview. Do you have any questions or final remarks to add?

Thank you for making the time to participate in my study.

----end------

APPENDIX D: Research analysis data association

Research Objectives	Research Questions	Propositions	Research Instrument Questions
Assess the level of concern and prioritization that organisations have on ransomware cyber-attacks;	Does financial institutions' cybersecurity strategy prioritize the threat of ransomware?	Ransomware is prioritised as a top risk as threat actors' motivation is heightened to exploit financial institutions	1. Ransomware is commonly understood as a form of malware that is designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors would then demand ransom in exchange for decryption. Would you then say that ransomware attacks are considered a top risk for senior management in your organisation? 2. Considering the current cyber-attack threat landscape, how big of a threat do you think Ransomware attacks are to South African Financial Institutions – specifically banking?

Investigate the key influences that contribute to a cyber-resilient posture of an organisation against ransomware attacks;	What are the factors that influence the cyber resiliency posture of a South African financial institution?	Components derived from the NIST framework (Identify, Protect, Detect, Respond and Recover) are key factors that influence cyber resiliency in financial organisations	4. In your view, what are the key factors or components that contribute to a cyber-resilient posture of an organisation against ransomware attacks?
Assess the role and influence of senior management in influencing the resilient posture against ransomware related cyber-attacks;	How can management's involvement in establishing a cybersecurity strategy accelerate the organisations' cyber resilience maturity?	Senior management have a critical role in ensuring cyber resiliency in financial institutions	8. In your view, what role do you think senior management should play in influencing the cyber resilient posture against Ransomware? 9. In your view, what can senior management do to accelerate the organisations' cyber resilience maturity to mitigate against ransomware?

Investigate how organisations can evaluate the effectiveness of cyber resilience as a mitigating strategy;	How can financial institutions assess how well their cyber resilience works as a mitigation strategy?	Various methods and techniques can be employed to evaluate the cyber-resilience of an organisation	3. In your view, how cyber resilient would you say is your institution against ransomware attacks? Prompt Question: how effective is the adoption of a cyber-resilience strategy in mitigating ransomware related attacks? 5. How can institutions evaluate if an adopted cyber-resilient strategy is effective at mitigating Ransomware attacks? 7. In your view, what needs to be in place to ensure that there is constant and consistent improvement of cybersecurity within organisations to mitigate against the ever-evolving threat landscape?

APPENDIX E: Ethical Clearance Certificate

Graduate School of Business Administration
University of the Witwatersrand, Johannesburg

Wits Business School

Wits Business School Ethics Committee
Constituted under the University Human Research Ethics Committee (Non-Medical)

Ethics Clearance Certificate

Ethics protocol number: WBS/DB2159255/202
This certificate is only valid with a legitimate ethics protocol number and signed by the Researcher (below).

Project title	Strategies to mitigate ransomware related cyber-attacks in South African financial institutions
Investigator / Researcher	Mrs Nqobile Mahlangu
Nature of Project	MM (Digital Business)
Decision of the Committee	Approved, provided stakeholders and participants are guaranteed confidentialty.
Issue Date of Certificate	2023-02-09
Expiry date	Date of submission of the project / research report
Chairperson	Dr Pius Oba ☎ +27 11 717 3976 +27 82 733 6587 ✉ pius.oba@wits.ac.za

---

Declaration by Researcher

One copy must be signed by the Researcher and returned to the Chairperson of the Wits Business School Ethics Committee.

I fully understand the conditions under which I am authorized to carry out the abovementioned research and I guarantee to ensure compliance with these conditions. Should any departure to be contemplated from the research procedure as approved I undertake to resubmit the protocol to the Committee.

Signature

09 FEBRUARY 2023
Date: