Stakeholders' perspectives on factors influencing the operationalisation of cyber resilience – A financial services case study

A research dissertation presented to the Department of Information Systems University of Cape Town

By

Asterico Adams

(ADMAST001)

in partial fulfilment of the requirements for the award of the degree of

Master in Commerce: Information Systems

June 2024

Supervisor: Professor Wallace Chigona

Co-supervisor: Dr Karen Sowon

University of Cape Town

The copyright of this thesis vests in the author. No quotation from it or information derived from it is to be published without full acknowledgement of the source. The thesis is to be used for private study or non-commercial research purposes only.

Published by the University of Cape Town (UCT) in terms of the non-exclusive license granted to UCT by the author.

University of Cape Town

Declaration

1. I know that plagiarism is wrong. Plagiarism is to use another's work and pretend that it is one's own.
2. I have used the APA convention for citation and referencing. Each contribution to, and quotation in, this research dissertation, *Stakeholders' perspectives on factors influencing the operationalisation of cyber resilience – A financial services case study,* from the work(s) of other people has been attributed, and has been cited and referenced.
3. This research design assignment, *Stakeholders' perspectives on factors influencing the operationalisation of cyber resilience – A financial services case study,* is my own work.
4. I have not allowed, and will not allow, anyone to copy my work with the intention of passing it off as his or her own work.
5. I acknowledge that copying someone else's work, or parts of it is wrong and declare that this is my own work.

Signature:

Signed by candidate

Full Name of Student: Asterico Adams
Student Number: ADMAST001

Date: 12 June 2024

Acknowledgements

To my supervisors, Professor Wallace Chigona and Dr Karen Sowon, thank you for your guidance, patience and valuable time you have spent with me on this incredible journey. I have nothing but the utmost respect for both of you and will always be thankful for your support and advice over the past year.

I would like to thank my company for allowing me to pursue this dream and for giving me the time and resources to make this a success.

To my late parents, Johanna and Reginald Adams, who always believed in the power of education and using education to shape the world around you. While you may not be here to celebrate this achievement with me, the lessons you taught me laid the foundation for this achievement.

Special thanks to my siblings, Reneel and Renelia, who always checked in on me during this journey and motivated me every step of the way.

Finally, and most importantly, to my wife Zulfa and son Aydin. Thank you for your motivation and support throughout the last two years. Thank you for sacrificing some of our time together, to allow me to complete this academic journey. This degree belongs to you both as much as it belongs to me and I will be forever grateful to both of you.

Abstract

Background: Cyber resilience provides organisations with the ability to continuously deliver business services during an adverse cyber event. However, due to the multidisciplinary and diverse operational requirements needed for cyber resilience, the operationalisation of such a concept can introduce layers of complexity within an organisation where operationalisation is dependent on multiple stakeholders. It is therefore imperative to understand stakeholder perspectives and how it contributes to successful cyber resilience operationalisation.

Purpose of the research: The objective of the study is to identify the factors that influence cyber resilience operationalisation from a stakeholder perspective and to explain how these factors impact the operationalisation of cyber resilience within an organisation.

Design/Methodology/Approach: The study employed qualitative methods and was guided by Linkov and Kott's cyber resilience matrix framework which breaks down cyber resilience to various phases, presented as a continuum: plan, absorb, recovery and adapt. A financial services organisation in the Western Cape was used as the case study and purposive sampling was used to identify and interview stakeholders within the financial services organisation and gain insight into their perspectives regarding cyber resilience.

Findings: The study underlined the influence of risk appetite and business requirements as factors in the plan phase, while the importance of data protection and adequacy of resilient system testing emerged as factors that influence the absorb phase. The impact of recovery time on business operations and data integrity were highlighted as key factors during the recovery phase. The impact of artificial intelligence, post incident review discussions and training and awareness were highlighted by stakeholders as important factors during the adapt phase. Overall, the findings show that these factors had an impact on the organisational priorities, resource availability, internal and external organisational considerations and on the need for continuous improvement of cyber resilience processes within the organisation.

Practical implications: The findings of this study highlight how these identified factors impact operationalisation considerations from a stakeholder perspective and how these considerations impact the cyber resilience readiness of the organisation.

Originality/Contribution: This study contributes to the research on the factors that play a role in cyber resilience operationalisation from a stakeholder perspective within a South African organisation and provides empirical evidence of how these factors impact the phases of cyber resilience. The outcome of this study can be used as a comparison against other industries.

Keywords: cyber resilience, operationalisation, stakeholders, perspectives, plan, absorb, recover, adapt.

Table of Contents

Table of Tables

List of Figures

1. Introduction

Cyberattacks have increased in occurrence and become more focused, targeted and refined in nature and have had enormous impact on the operational stability of organisations (Linkov & Kott, 2019; Hausken, 2020). The frequency of these cyberattacks were highlighted in a digital defense report produced by Microsoft, which reported that Microsoft technology had blocked an average of 4 000 password attacks attempts per second, while multi factor authentication (MFA) fatigue attacks, where repeated requests for MFA approvals target users using MFA for applications, were around 6 000 per day, for the period from July 2022 to June 2023 (Microsoft, 2023). The report further states that across the telemetry data collected by Microsoft during the same period, ransomware attacks had also increased by more than 200% since September 2022, and that there had been a significant rise in ransomware attacks targeting a larger range of countries and sectors.

Another study conducted by CISCO, reported that while 82% of the 6 700 respondents were anticipating a cyber incident to disrupt their business in the near future, only 15% of respondents were in a position to be resilient enough to mitigate and recover from cyber incidents (CISCO, 2023). The study also reported that the financial cost for companies that had disclosed a cyber incident during the period, had an average minimal loss of $500 000 (CISCO, 2023), which highlights the need for organisations to not only prepare and protect themselves against cyber threats, but also to build resilience to continuously delivery business services during an adverse cyber event.

To minimise the effect that these attacks have on operational stability, cyber resilience has emerged as a viable solution by focusing on the continuous delivery of business system operations through the adverse conditions brought on by a cyberattack (Björck et al., 2015; Bodeau et al., 2018; Annarelli & Palombi, 2021). While many organisations have business continuity and disaster recovery plans which cater for natural and man-made disasters, these plans do not cater for mitigating modern and sophisticated cyber based threats (Smith, 2023; Dickson & Goodwin, 2020; Assibi, 2023).

Both the CISCO and Microsoft reports emphasize the need for specific cyber resilience measures to be implemented which can help address the risks across the expanding digital organisational landscape and integrated connectivity points shared between organisations, staff and third parties (Microsoft, 2023; CISCO, 2023). These measures include protecting data, identities, systems as well as networks and embedding a collaborative risk culture, to ensure that these measures are not only seen as technical safeguards but also incorporating employees across the organisation to play a role in the operational functions.

Cyber resilience, however, is not a one size fits all. The measures to be implemented and how it should be implemented is dependent on the organisation's context such as size of the organisation, sector, digital maturity and operational structure (Tsen, Ko & Slapnicar, 2022). Thus, to ensure that an organisation can benefit from cyber resilience, specific operationalisation of such a solution is required to ensure that the organisational objective of cyber resilience is achieved (Linkov & Kott, 2019; Bodeau et al., 2018). In the context of this research, operationalisation refers to the process of translating the various aspects of cyber resilience into realities that make sense for the organisation. It is ensuring that best practice solutions can be translated from recommendations into practice and that through the practice of operationalisation, the organisation can operate in a specific manner which supports the overall goal of cyber resilience. This integrated approach incorporates operational processes and resources from across the organisation such as Information Technology (IT) and operational risk management processes, business strategy and continuity objectives, incorporation of various technical resources, governance and training programmes (Dupont, 2019; Estay et al., 2020, Loonam et al., 2020; Hausken 2020; Annarelli & Palombi, 2021).

Research has however highlighted the challenges of implementing cyber resilience and these challenges include embedding or complimenting the existing processes with the required governance and oversight, ensuring the correct systems are selected to form part of business continuity, training and awareness of the tasks that need to followed during an actual adverse cyber event, as well as technical and financial resources to support the practical application towards operationalisation within an organisation (Davidson et al., 2016; Carías et al., 2020; Loonam et al., 2020; Tsen, Ko & Slapnicar, 2022). As a result of having such a multidisciplinary approach to cyber resilience, the interpretation of operationalisation across multiple, diverse organisational disciplines can further complicate the understanding of the operationalisation process (Carías Alvarez, 2021; Davidson et al., 2016; Greiman & Bernardin, 2021).

Due to the complexity associated with assembling all the resources and processes together within an organisation, the importance of stakeholders has been emphasized in research as a significant factor in ensuring the successful integration of these various operational elements to support the objective of cyber resilience (Tsen, Ko & Slapnicar, 2022; Chatterjee, 2021; Bodeau & Graubart, 2013; Dupont et al., 2023). Stakeholders are viewed as key decision makers who have influence in providing strategic direction within organisations through oversight and accountability for decisions (Werth, 2019; Freeman & McVea, 2001; Loonam, 2020). In the context of this study, stakeholders are employees of the organisation who have the responsibility of operationalising cyber resilience.

For stakeholder contributions to be effective, their perspectives regarding factors that influence cyber resilience are of great value within an organisational setting, as it provides a basis through which the different operational elements within an organisation can work together to achieve the objective of cyber resilience (Carías Alvarez, 2021; Annarelli & Palombi, 2021; Chatterjee, 2021).

1.1 Problem Statement

Due to the nature of cyberattacks, many organisations are searching for a pragmatic solution to resilience, through the adoption of processes that can provide operational availability of key business systems (Pavao et al., 2022; Linkov & Kott, 2019). The financial sector is specifically prone to cyberattacks, with an increase in ransomware attacks from 55% in 2022 to 64% in 2023 (Sentinel One, 2023) and a significant increase in cyber-attacks against the financial sector globally which saw a 28% higher average in data losses than other industries (IBM, 2023).

To mitigate these risks associated with financial crime, especially in the digital age, financial organisations focus on the implementation and management of suitable cyber security culture and operational resilience controls (Dupont, 2019; Uchendu et al., 2021). Literature highlights the challenges associated with cyber resilience operationalisation due to diverse organisational processes and the involvement of many different stakeholders within the organisation. (Pavao et al., 2022; Linkov & Kott, 2019).

As a result of the diverse perspectives of stakeholders, the organisation may encounter significant challenges and barriers, such as conflicting priorities, lack of appropriate resource allocation and adequate focus, impeding its effectiveness in operationalising cyber resilience. These challenges often result in misaligned controls, lack of trust amongst stakeholders and additional strain on the existing processes (Bagheri, 2020) which could negatively impact the intended outcome for the organisation to continuously deliver business services (Ferdinand, 2015; Davidson et al., 2016; Greiman & Bernardin, 2021). In this regard, the perspectives of stakeholders play a key role, as it ensures that the actions of these stakeholders contribute to the overall goals and objectives of the organisation (Freeman & McVea, 2001; Werth, 2019) and success of implementing cyber resilience.

From a research perspective, this case study can provide insight into the perspectives of the various stakeholders within a financial organisation being used a case study and identify how these perspectives contribute to the forming of decisions regarding the allocation of resources, organisational priority and focus on resilience. The insight garnered from these perspectives can assist with identifying the impact these factors have on the organisational processes within the financial organisation which support cyber resilience.

1.2 Research purpose and objectives

The purpose of this study is to gain a greater understanding of which factors influence cyber resilience operationalisation in the financial services sector. We do this from a stakeholder perspective where we analyse perspectives about cyber resilience from various stakeholders within a single organisation. Through the adoption of a qualitative approach, using a semi-structured interview process as a primary data collection medium, the research aims to provide insight into stakeholder perspectives on which factors influence cyber resilience operationalisation within an organisation.

The main question the research seeks to answer is: **What factors influence how cyber resilience is operationalised within organisations?**

The following sub questions and corresponding objectives were formulated to help answer the main research question and is referenced in Table 1.1.

Table 1.1: Research sub questions and objectives

Question	**Objective**
What factors influence cyber resilience operationalisation?	To explain which factors influence cyber resilience operationalisation.
How do these factors influence stakeholder perspectives and practices with regards to cyber resilience?	To explain how these factors influence stakeholder perspectives and practices with regards to cyber resilience.
How do the factors and stakeholder perspectives influence the operationalisation of cyber resilience within an organisation?	To explain how these factors and stakeholder perspectives impact cyber resilience operationalisation within an organisation.

1.3 Research Context and Approach

Several studies have shown that the industry where an organisation is embedded, influences the stakeholder actions which need to be undertaken (Linkov & Kott, 2019; Neeme, 2022; Werth 2019). A financial organisation therefore provides a useful case for the study. First, when reviewing contextual factors associated with a specific type of industry, the financial or consumer-oriented industries are consistently highlighted in research as valuable sources of research information mainly due to the stringent compliance and regulatory requirements which require cybersecurity measures to be in place (DuPont, 2019; Neeme, 2022; Dupont et al., 2023).

Second, financial organisations also store financial and personal information, transactional data, confidential supporting documentation and intellectual property which are valuable to threat actors and in turn heightens the risk associated with financial organisations (DuPont, 2019). Taking these risk factors into account, a financial services organisation offers a suitable case study for this research, as there is a higher probability of existence of security controls required within the financial sector which lends itself to the concept of cyber resilience.

While there have been numerous studies on cyber resilience, most have been in the context of developed economies that are starkly different from developing countries in their access to resources to manage cyber-attacks. This study therefore considers cyber resilience in an African context, as the rise in technology and internet adoption in Africa, has also seen in increase in cyber threats (Dalton, van Vuuren & Westcott 2017; Liquid Technologies, 2022). Being one of the countries at the forefront of technology and internet use in Africa, South Africa has faced an increasing number of cyberattacks over the past decade (Pieterse, 2021; Peter, 2017) which has led to a focus on cyber risk, cyber security and resilience controls (Dalton, van Vuuren & Westcott 2017; Sithole, 2019; Peter, 2017).

Based on the context of the developing country such as South Africa, a financial organisation within the Western Cape was chosen as the case study to enable the answering of the research questions and objectives.

1.4 Significance of the study and Structure of Thesis

This study contributes to the body of knowledge of stakeholder perspectives regarding cyber resilience by studying stakeholder perspectives towards cyber resilience within an organisational setting in the Western Cape. The outcomes of this research could provide useful insights for researchers who study the area of cyber resilience operationalisation within the financial services industry, as well as stakeholders or interested individuals who may be considering operationalising cyber resilience within their own organisations.

The following section outlines the structure of this thesis, with a brief explanation about the contents of each chapter.

- **Chapter 2**: Literature review section provides a review of the existing literature regarding the definition of a stakeholder and the impact of stakeholder perspectives on information technology implementation. The chapter continues by defining the concept and impact of cyber resilience, while also explaining the differing aspects of cyber resilience and cyber security, as well as cyber resilience operationalisation.
- **Chapter 3**: The theoretical framework chapter provides an overview of the chosen theory which is used to support this study and this case. The cyber resilience matrix framework has been chosen as a lens to guide this study.
- **Chapter 4**: Research design presents the research methods that have been employed during this study to enable the researcher to answer the research question.
- **Chapter 5:** Research findings section discusses the findings of the research and the main themes that emerges from the data analysis process.
- **Chapter 6**: Discussion and conclusion provides a succinct summary of the findings, limitations of the research and proposed future research.

2. Literature review

This chapter situates the study within the wider body of literature and reviews the main strands of literature related to this study. First, the chapter provides an overview of stakeholder research by defining what a stakeholder is and the impact of stakeholder perspectives on information technology implementation. This is followed by defining the concept of cyber resilience and providing an overview of the differences between cyber resilience and cyber security. The chapter then concludes by describing the cyber resilience operationalisation process.

2.1 Overview of stakeholder research

2.1.1 Defining the concept of stakeholders

The concept of stakeholders is well documented throughout several research studies within literature over the past few decades (Freeman, 1984; Donaldson & Preston, 1995; Bryson, 1995; Florea & Florea, 2013; Mishra & Mishra, 2013). While the term, stakeholder, have a few varying definitions throughout literature, one of the consistently attributed aspects of a stakeholder is described as participants who hold a stake in decisions made by an organisation or have influence on decision making which can have an impact on the goals of the organisation (Freeman & McVea, 2001; Werth, 2019).

These aspects have their definitions rooted in the early iterations of the concept of a stakeholder, which focus on the premise that the actions of a business or organisation have an impact on both internal and external environments (Freeman & McVea, 2001; Beaver, 1999). This is demonstrated by the fact that organisations form part of an ecosystem within industries and are therefore deemed as role players within the industry they operate in (Florea & Florea, 2013; Machan, 2017; Werth,2019) and that all actions undertaken by an organisation has an effect in the industry in which they operate, and these actions in turn have a ripple effect on society (Florea & Florea, 2013; Frooman, 1999). Stakeholders can be identified as internal to an organisation and consist of employees, senior management and shareholders or they can be identified as external to an organisation in the form of customers, service providers, the general public and more (Donaldson & Preston, 1995; Florea & Florea, 2013).

Taking into the account the influence stakeholder actions have on both external and internal environments, Freeman, proposed the most widely known and used definition of a stakeholder which states, "A stakeholder in an organisation is (by definition) any group or individual who can affect, or is affected by, the achievement of the organisation's objectives" (Freeman, 1984, p.146). Based on this definition of a stakeholder proposed by Freeman (1984), every organisation will have a group structure or people who affect or are affected by the decisions made within an organisation.

This definition of a stakeholder, which depending on the structure of the organisation, will influence and impact the strategy and direction of an organisation through its decision-making processes (Werth, 2019).

Literature provides alternative definitions of stakeholders such as the following; "Those individuals or groups who depend on the organisation to fulfil their own goals and on whom, in turn, the organisation depends" (Johnson, Scholes & Whittington, 2002, p.165) or as cited by Bryson (1995, p.27) "Any person, group or organisation that can place a claim on the organisation's attention, resources, or output, or is affected by that output." However, these definitions incorporate the important elements of the definition proposed by Freeman (1984), which focus on the effect a stakeholder has on the organisation and its influence on strategy (Werth, 2019) and the researcher has therefore opted to use the definition proposed by Freeman as the working definition in this paper.

The type of actions or decisions taken by stakeholders have also evolved over the past few decades from not just being purely focused on growing the financial success and shareholder gains but includes introducing value creation and long-term sustainability (Sanders & Bell, 2007; Freeman & McVea, 2001). The shift in moving away from only creating financial gain is attributed to the changing business environment where sustainability and creation of a society driven business ecosystem, are key to the long-term survival of an organisation (Freeman & McVea, 2001; Werth, 2019; Harrison & Van der Laan Smith, 2015).

A fundamental part of the long-term survival of an organisation, is the ability to build organisational resilience, which provides a sense of trust to investors, customers and suppliers that an organisation can adapt to unforeseen circumstances (Ma, Xiao & Yin, 2018). Due to the acceleration of organisations who operate within the e-commerce and online ecosystems, organisational resilience has extended beyond the traditional risk scenarios and includes having a strategy to deal with the impact that cyber threats pose to an organisation (Ma, Xiao & Yin, 2018; Dupont, 2019).

2.1.2 Stakeholder perspectives in information system implementation

Stakeholders play an important role in contributing towards organisational resilience by ensuring a shared vision that has a clear purpose is clearly articulated and actioned (Munusamy & Khodadi, 2023). Building such organisational resilience, does however require the input of various stakeholder perspectives to ensure a uniformed and shared approach and this is no different when dealing with IT risks associated with cyber threats (Ma, Xiao & Yin, 2018).

One of the key factors that plays a role in the decision-making thought process for stakeholders, is their perspective regarding a specific concept or topic (Scolobig & Lilliestam, 2016). Perspectives often provide the foundation from which key decisions or actions are taken by stakeholders within an organisation and this is an especially important aspect of decision making as it impacts a significant part of the operations of an organisation (Reed, 2008; Haki, Aier & Winter, 2016).

Stakeholder perspectives are widely seen as beneficial to an organisation, as it increases the probability of implementation, the quality of the outcome of decisions and lends credibility to the legitimacy of a decision and therefore contributes to the overall action taken by a stakeholder (Scolobig & Lilliestam, 2016; Crane, 2020). Stakeholder involvement provides the required leadership oversight to ensure commitment to implementations but can also constrain an organisation due to the conflicting and competing interests of various stakeholders (Haki, Aier & Winter, 2016).

The importance of stakeholder involvement and support has also been noted as critical to the success of IT implementations (Munusamy & Khodadi, 2023; Bagheri, Ridley & Williams, 2023). IT implementation refers to the introduction of new technology into existing processes within an organisation and how the technology interacts within the organisation (Harper & Utley, 2001). Once implemented, IT adoption is then seen as the buy-in and continued use of the solution by the users within the organisation (Kim & Crowston, 2011).

There are however several challenges that are associated with IT implementation due to the multifaceted approach to IT implementation which spans across different boundaries within an organisation, with diverse sets of stakeholders, each with their own perspective and interests in different guidelines, policies and standards (Haki, Aier & Winter, 2016). These challenges include the allocation of time and resources to the project, dedicated focus for duration of implementation and (Tarhini, 2015; Scolobig & Lilliestam, 2016; Sithole, 2019). While there is potential for innovative collaboration to ensure implementation is a success, the potential for conflict, unproductivity and is higher as a result of the various expertise, views and interests of the stakeholders (Haki, Aier & Winter, 2016; Tarhini et al., 2015; Crane, 2020).

As cyber resilience is a multi-disciplinary and collaborative effort, stakeholder perspectives are a key element that drive decisions which impact the overall operationalisation of cyber resilience within an organisation. It is therefore crucial to understand the perspectives held by stakeholders, to enable a cooperative dynamic, which positively contributes to the intended goal of the IT implementation within an organisation (Bagheri, Ridley & Williams, 2023; Haki, Aier & Winter, 2016; Boonstra, 2006).

2.2 Cyber resilience operationalisation

2.2.1 Global issues facing cyber security

Organisations have become increasingly reliant on adopting technologies that provide competitive advantages and maintaining their relevance in the ever-changing interconnected market (Munusamy & Khodadi, 2023). However, with these shifts into the digital landscape, many organisations are exposed to increased cyber risk which come in the form of operational disruption, financial loss and data breaches (Dupont, 2019; (Munusamy & Khodadi, 2023).

Surveys conducted by Deloitte and Ernst and Young in 2019 stated that despite the efforts from industries focussing on cyber security as a top priority, there were still a considerable number of breaches being reported, which indicated little improvement in addressing the organisational concerns when it comes to cyber security (Tsen, Ko & Slapnicar, 2022). More recently, the Microsoft digital defense and CISCO security readiness reports released in 2023, indicate the alarming growth and sophistication of cyber attacks as a major concern for many organisations globally.

The Microsoft digital defense report highlights the increase of human operated ransomware attacks, password based attacks and open-source attacks, which spiked 742% since 2019 (Microsoft, 2023). These attacks underscore the frequency and proliferation of attacks that overwhelm organisations and that are becoming more difficult to detect and protect against. The CISCO security readiness report state that financial services organisations remain a top target for threat actors based on the sensitive information stored by these organisations and the report further emphasises the need for additional layers of security to combat these evolving digital threats (CISCO, 2023).

These reports underline the issues facing organisations globally when dealing with the threat of cyber attacks. These include an arrangement of attacks aimed at users, who are often seen as the weakest link in the cyber security ecosystem (Fischer-Hübner et al., 2021), while preventative security controls only focus on a certain area within the organisation deemed as high risk and may not sufficiently address other areas that could also be prone to cyber attacks (Bagheri, 2020).

Taking all these issues into account, it becomes clear that organisations are in need of more solutions to supplement the cyber security strategies in place within an organisation. It is therefore important for organisations to focus on additional controls that can complement the existing preventative cyber security control frameworks to form a more cohesive, pragmatic approach to combatting the effects of cyber attacks.

2.2.2 Defining the concept of cyber resilience

To counter the effect of cyber risk, organisations have adopted several different layers of cyber security controls to manage cyber risk. While cyber security controls provide organisations with a form of assurance, these security controls mostly focus on the protection and prediction element of recognisable cyber threats and may not be effective against the fast changing and evolving nature of the threat landscape (Munusamy & Khodadi, 2023; Dupont, 2019; Refsdal, Solhaug & Stølen, 2015).

To compliment these security controls, cyber resilience has emerged as viable solution for organisations who want to ensure the operational functionality of their core systems during, and after, the advent of a cyberattack.

The foundational basis of cyber resilience, which focuses on a systematic way to remain operational despite adverse conditions, draws its operational elements from the practice of resilience. One of the most widely accepted definitions of resilience, is that of The National Academies of Science, which defines resilience as the "*the ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events*" (National Research Council, 2012, p.16).

This definition draws elements from other resilience discipline definitions, to provide a holistic dimension through which phases such as planning and preparation, absorption, recovery and adaption all contribute towards ensuring the intended outcome of resilience is achieved (Connelly et al., 2017). In Table 2.1, the resilience phases are mapped according to four phases namely, plan, absorb, recover and adapt.

Table 2.1: NAS phases of resilience based on application domains (National Research Council, 2012)

NAS phase of resilience	Resilience Feature	Description by Application Domain			
		Socio-Ecological	**Psychological**	**Organisational**	**Engineering & Infrastructure**
Plan	**Critical Functions (Services)**	A system function identified by stakeholders as an important dimension by which to assess system performance			
		Ecosystem services provided to society	Human psychological well-being	Goods and services provided to society	Services provided by physical and technical engineered systems
Absorb	**Thresholds**	Intrinsic tolerance to stress or changes in conditions where exceeding a threshold perpetuates a regime shift			
		Used to identify natural breaks in scale	Based on sense of community and personal attributes	Linked to organisational adaptive capacity and to brittleness when close to threshold	Based on sensitivity of system functioning to changes in input variables
Recover	**Time (and Scale)**	Duration of degraded system performance			
		Emphasis on dynamics over time	Emphasis on time of disruption (i.e., developmental stage: childhood vs adulthood)	Emphasis on time until recovery	Emphasis on time until recovery
Adapt	**Memory/Adaptive Management**	Change in management approach or other responses in anticipation of or enabled by learning from previous disruptions, events, or experiences			
		Ecological memory guides how ecosystem reorganizes after a disruption, which is maintained if the system has high modularity	Human and social memory, can enhance (through learning) or diminish (e.g., post-traumatic stress) psychological resilience	Corporate memory of challenges posed to the organisation and management that enable modification and building of responsiveness to events	Re-designing of engineering systems designs based on past and potential future stressors

Cyber resilience has multiple definitions defined in literature across the past number of years. Some of the earlier definitions of cyber resilience focus on the transitionary state of stability and balance within systems (Haimes, 2009), while within other studies, cyber resilience is broadly defined as the ability to anticipate, withstand and recover from a cyber-event (Dalton, van Vuuren & Westcott, 2017; Dupont, 2019; Bodeau et al., 2018). This definition has a focus on the ability to anticipate the adverse event, plan for it through implementation of measures and recover in the event of failure. In certain instances, there is a focus on adapting to future threats as part of a post incident review perspective (Bodeau et al., 2018; Linkov & Kott, 2019).

Drawing from the National Academy of Sciences resilience definition, Björck et al. (2015) defined cyber resilience as the ability to deliver the anticipated outcome of a system, despite the adverse cyber effects on the system. This definition provides a multi-dimensional approach to cyber resilience by ensuring the organisation can address the resilience characteristics to plan, absorb, recover and adapt from cyberattacks. This definition proposed by Björck et al. (2015) for cyber resilience is aligned to the concept of resilience and suitable for the purpose of this literature review as it addresses the resilience characteristics from a holistic organisational perspective, as these organisational requirements can be mapped generically to each phase of cyber resilience (Estay et al., 2020; Hausken, 2020; Annarelli & Palombi, 2021).

2.2.3 The Stages of Cyber Resilience

Cyber resilience as defined by NAS has four main phases (Table 2.1). These phases consist of the plan, absorb, recover and adapt phases. These four phases work together as an integrated, holistic process that support the concept of cyber resilience.

2.2.3.1 Plan phase of cyber resilience

The planning phase is the cornerstone of the operationalisation process and is a key step in ensuring that an organisation can plan and prioritise the resources required to effectively build a cyber resilience plan. During this phase, stakeholders from across the organisation are identified, who would be instrumental to the implementation of the cyber resilience strategy and operationalisation of processes that support the objective of cyber resilience (Annarelli, Nonino & Palombi, 2020; Mishra & Mishra, 2013). Once stakeholders are identified, the identification of the type of risks which impact the organisation is performed through various iterations of risk assessments such as business impact analysis, cyber risk and operational risk assessments, which forms part of a broader risk management practice (Pavao et al., 2023; Linkov et.al, 2013; Carías et al., 2020). During the risk management process, both internal and external risks are identified, documented and classified, to determine priorities from a

system and operational process level and develop risk mitigation strategies to address the risk threshold (Carías et al., 2020; Refsdal, Solhaug & Stølen, 2015)).

The risk management process is crucial to the planning and absorb phase of cyber resilience as it directly addresses the types of risks that the organisation might face and how to remediate those threats (Carías et al., 2020; Linkov et al., 2013; Collier et.al, 2014). The remediation tasks would include the co-ordination of the cyber resilience operationalisation process across the impacted business areas within an organisation and have a big focus on the technical aspects of the identified systems (Linkov et al., 2013; Estay et al., 2020).

The results of these integrated risk assessments provide the organisation additional information regarding which systems and its connected business processes, are prone or vulnerable to the identified cyber threats (Annarelli & Palombi, 2021). Technical resources are assigned to unpack and validate the results of the assessments from a technical perspective, to investigate whether business critical systems, their integrated services and underlying infrastructure, are able to handle the type of cyber threats identified during the risk management process.

2.2.3.2 Absorb phase of cyber resilience

Cyber risk assessments are designed to focus on the probability and impact of cyber threats and many of these cyber threats have a technical attack vector associated with them which requires organisations to understand the technical impact of these cyber threats on the identified systems (Burstein et al., 2012; Loonam et al., 2020). The absorb phase utilises the contextualised outputs of the risk management process, to technically prepare the identified critical business systems to withstand the impact of these cyber threats (Linkov & Kott, 2019; Dupont, 2019).

One of the most important aspects of the absorb phase is ensuring that the risk mitigation steps, which include the operational processes and technical control implementations, are tested to ensure that the organisation can absorb or withstand the impact of a cyber threat (Dupont, 2019). A study conducted by Tsen, Ko & Slapnicar (2022) stated that the higher severity of a cyber breach, the higher the likelihood of investigations, which could lead to penalties and regulatory fines. Due to the amount of customer information and payment data customer facing organisations store for processing, the importance of data protection also plays role a during the absorb phase to ensure that data is kept safe and secure within business-critical systems (Tsen, Ko & Slapnicar, 2022; Brunetti et al., 2020).

The study also emphasizes the fact that organisations in critical industries better defend themselves with the controls that are in place, through deployment of practical prevention, detection and recovery mechanisms and that the strength of these controls require continuous testing and simulation exercises.

These simulation exercises, which are technical in nature, are driven by technical resources and the associated test plans are tested according to the various cyber threat scenarios which are determined through the risk assessments (Annarelli, Nonino & Palombi, 2020; Linkov & Kott, 2019). These technical tests would include vulnerability scans to look at potential technical vulnerabilities within the infrastructure of system, penetration tests which provide an objective third party perspective of the threat and detection response rates, to ensure that the process to detect the threats are aligned to the risk appetite of the organisation (Linkov & Kott, 2019).

2.2.3.3 Recovery phase of cyber resilience

The recovery phase refers to the point at which a system has adequately recovered to a working state and is usually measured by recovery time objectives, in conjunction with the risk levels assigned to business-critical systems during the risk management phase (Pavao et al., 2023). The recovery time objective would be the agreed amount of time which would meet the risk appetite of the organisation and be measured as the amount of time required to ensure continuous business delivery. This phase is designed to ensure that the systems can actively recover to a working state and continue in that state to ensure the overall objective of cyber resilience.

This phase is usually categorised by the technical process to recover the system and would include system design steps, which run in a sequential order to ensure that the system is brought back online in safe state. This phase is very similar to the way disaster recovery would invoke business continuity process and may include running parallel systems, streamlining system functionality to only deliver the most critical services which can enable continuous business delivery of services (Linkov & Kott, 2019) or invoking an isolation process that encloses the part of the system that experiences the impact of a cyber event occurs and provides business the required time to focus on continuing operations. (Annarelli, Nonino & Palombi, 2020).

2.2.3.4 Adapt phase of cyber resilience

Once the system is recovered to a working state and the cyber threat has been contained, a post incident feedback process is initiated which provides feedback regarding the entire operationalisation process. This process is used as a mechanism to continually mature the cyber resilience practice within an organisation by ensuring that actions or aspects that are

highlighted as a failure or inadequate, be noted and addressed by the various stakeholders (Annarelli, Nonino & Palombi, 2020; Neeme, 2022).

These actions are crucial for any organisation to stay abreast of the evolving cyber threat landscape. Action items may include using the knowledge collected from the cyber event, to assist with better technical preparation which could result in different configurations being tested on systems (Linkov et al., 2013) and the amendment or introduction of various protocols to expedite processes to support quicker resolution times (Bagheri, Ridley & Williams, 2023). There may also be changes to the type of resources that are assigned to systems and could also include the introduction of additional training across some of the identified areas to ensure uniformed understanding and focus on operational duties (Jeimy & Cano, 2023; Dupont, 2019; Annarelli, Nonino & Palombi, 2020).

The adapt phase also provides an organisation with the opportunity for stakeholders to communicate with each other during this joint review and focus on the organisational objective (Bagheri, Ridley & Williams, 2023). Communication allows for better understanding of the different processes which may be managed by several different stakeholders from differentiating backgrounds, leading to a more uniformed approach which all forms part of the objective of this adapt phase, which is to become more cyber resilient against evolving cyber threats (Carías Alvarez, 2021; Annarelli & Palombi, 2021).

2.2.4 How Cyber resilience differs from cybersecurity

The concept of cyber resilience is occasionally interchangeably used with that of cyber security however, there are several characteristics that differentiate the two concepts from one another (Hausken, 2020; Estay et al., 2020). Björck et al. (2015) provides a differentiating view of the characteristics of cyber resilience and cyber security based on varying aspects such as the objective, intention, approach, architecture and scope of cyber resilience. These characteristics, defined in Table 2.2, align to the definition and objective of resilience and provide organisations with a general understanding of which aspects need to be considered when adopting cyber resilience within the organisation (Linkov & Kott, 2019). These characteristics can also be used to differentiate between the two concepts of cyber resilience and cybersecurity, paving the way for a better understanding of how integrated the process within the organisation is, instead of it being assigned as a singular responsible function (Dupont, 2019; Zemba et al., 2019).

Table 2.2: Characteristics of Cybersecurity and Cyber resilience (Björck et al., 2015)

Aspect	Cybersecurity	Cyber Resilience
Objective	Protect IT systems	Ensure business delivery
Intention	Fail-safe	Safe-to-fail
Approach	Apply security from the outside	Build security from within
Architecture	Single layered protection	Multi layered protection
Scope	Atomistic, one organisation	Holistic, network of organisations

The following section provides a high-level overview of the differentiating characteristics of cyber resilience based on the five aspects of objective, intention, approach, architecture and scope.

2.2.4.1 Continuous business delivery

The objective of cyber resilience is to ensure business delivery through continuous availability of services, despite the adverse conditions. The enablement of such availability provides additional value to the organisation through continuity and therefore ensuring less impact on revenue and value generation (Hausken, 2020). This value can however only be derived by an organisation, if the critical systems have been identified through a cyber-risk management process and included as part of the cyber resilience process. This process would include the development of metrics to measure resilience from both a performance and cost perspective (Graubart & Bodeau, 2016). From that perspective, it is imperative to include participation from business stakeholders, and not just IT teams, so that systems deemed in scope for cyber resilience, are aligned to the business objectives of an organisation (Carías et al., 2020). That allows for the integration of business objectives within the cyber resilience adoption process and provides strategic insight to senior stakeholders whose buy-in and participation is required (Dupont, 2019; Estay et al., 2020, Loonam et al., 2020).

2.2.4.2 Safe to fail design

Safe to fail, as a technical concept, requires a system to be able to run as intended while withstanding the effects of cyber events. Studies also position the ability to fail in a controlled manner, as part of the safe to fail concept, as it forms part of the ability of the system to respond and recover (Annarelli, Nonino & Palombi, 2020; Carías et al., 2020; Zemba et al., 2019). To enable this, bespoke and customised systems should be built with the intention of the safe to fail concept and requires resources familiar with these systems to be able to independently test applicable safe to fail scenarios (Annarelli & Palombi, 2021).

Since safe to fail is a crucial component of the cyber resilience concept, factors such as development time, skilled resources and technology acceptance must be considered as part of this (Graubart & Bodeau, 2016; Colabianchi, 2021).

2.2.4.3 Build security within

The aspect of building security within is a multi-dimensional approach that involves the collaboration of information technology systems, applications and business operations as part of resilience. In this instance, resilience is built in as part of business process, rather than an add on and through this, mitigates the risk of resilience being seen as a singular function (Björck et al., 2015). Through this lens, resilience can be included in business processes to support the overall objective of cyber resilience by ensuring that awareness and guidelines about cyber resilience process is well documented and communicated within the organisation (Hausken, 2020; Colabianchi, 2021). By enabling security to be built from within the organisation, awareness is raised amongst not only stakeholders but also process owners and individuals who are responsible for daily operational duties (Carías et al., 2020). Through this type of collaboration, there is a better understanding of what cyber resilience is and how the amended process supports the operationalisation process.

2.2.4.4 Multi layered protection

The architecture aspect of this cyber resilience characteristic is a multi-layered protection layer approach, where several layers are designed to support the safe to fail aspect. Instead of one layer being used as a form of secure design, a layered approach is used to enforce better security (Annarelli & Palombi, 2021). This also allows for a suitable recovery mechanism at each layer, which well suited for the recovery phase in cyber resilience. Server clustering, three-tiered network layers and micro services architecture are some of the examples of how a layered approach would be implemented and managed as part of cyber resilience (Bodeau et al., 2018). One of the factors that would influence multi layered protection is overhead and cost to maintain multiple layers of protection. A return on investment and derived value analysis is required during the planning phase of multi layered protection (Linkov & Kott, 2019).

2.2.4.5 Holistic, network of organisations

The interconnected nature of business is an important factor to consider as the cyber threat can originate from any number of interconnections both internally to an organisation and externally through suppliers and service providers (Linkov & Kott, 2019; Annarelli & Palombi, 2021). The approach to mitigate both internal and external risks, requires specialised skills and technological resources, as well as costs, to monitor and manage network services and help establish a baseline of normal traffic traversing a network. In this scenario, stress tests can be conducted to understand the volume a network traffic route can absorb before some sort of redundancy of failover measures can be implemented to allow for minimum interruption during an attack or recovery process (Björck et al., 2015). This type of testing is required on both internal and external network routes, to ensure that all connections are adequately tested as part of resilience and that measures are put in place to ensure a holistic view of entry points in and out of the organisation are accounted for.

2.2.5 Cyber resilience in the context of financial institutions

As the financial sector has transformed and adapted to the rapid adoption of digital financial services, the rate of cyber threats has also increased (Dupont et al., 2023; Maurer & Nelson 2020). With the increase in cyber threats, financial institutions have had to adjust cyber security measures and strategies to counter the threat posed by these cyber threats and adopt resilience strategies to ensure a more integrated approach to the ubiquitous nature of these threats. (Pomerleau & Lowery 2020; D. L. Carter, 2017; Dupont, 2019; Dupont et al., 2023). This has seen an increase in the number of cyber resilience strategies being explored and implemented by financial institutions (Maurer & Nelson 2020; Dupont et al., 2023) and has seen the European Union introduce an operational resilience act to enable a uniformed approach to the way cyber resilience requirements can be measured in financial institutions and third parties (Clausmeier, 2023). This act, which seeks to be implemented in 2025, highlights the importance of cyber resilience for financial institutions.

2.2.6 Cyber resilience operationalisation

As presented in section 2.2.3, there are several characteristics that demonstrate the multi-disciplined and integrated nature of cyber resilience. For the concept of cyber resilience to be successful within an environment, the operationalisation process needs to be defined and understood by all individuals involved in the daily organisational activities (Dupont et al., 2023; Linkov & Kott, 2019). As referenced in the introduction in chapter 1, operationalisation refers to the process of translating a concept into practice within an environment (Iyamu & Batyashe, 2020). Through operationalisation, the organisation operates in a specific manner which supports the overall goal of cyber resilience.

This approach provides the organisation and stakeholders with a way to operationalise and integrate the cyber resilience concept into day-to-day operational activities of the organisation, through the active participation of the required resources (Iyamu & Batyashe, 2020).

To effectively guide organisations with an approach to operationalisation, there are several research studies that have proposed numerous cyber resilience frameworks over the years (Pavão et al., 2023). Since there is no universally applicable framework, organisations can tailor these existing frameworks to their organisational requirements as these frameworks can vary in approach. These approaches range from technical implementations based on certain technically focused controls and system thresholds, to a risk-based approach based on the risk appetite of the organisation. Annarelli & Palombi (2021) highlighted several examples of cyber resilience frameworks in a paper that briefly described the varying approaches to operationalisation.

An example of a risk-based cybersecurity framework proposed by Collier et al. (2014) positions a dynamic and adjustable risk-based approach that takes the surrounding organisational environment into account, when developing risk assessment models. These models incorporate any new knowledge of the organisation environment to inform and update decision making models that improve cyber security and cyber resilience processes (Collier et al., 2014). By enabling continuous feedback into the risk management lifecycle, this risk-based approach offers an effective threat management process, while ensuring that risks highlighted and managed within the organisation are continuously tracked. In instances where these risks evolve or stakeholder priorities change, these changes are incorporated in the process of operationalisation by adapting resilience capabilities within the organisation (Collier et al., 2014).

On a more technical level, a technical focused framework is the STRATUS framework which stands for Strategic and Tactical Resiliency Against Threats to Ubiquitous Systems. It is a resource based, technically constructed focused model that takes the vulnerability and reliability levels of hardware and software resources into account when analysing distributed threats and using this information to respond to such threats (Burstein et al., 2012). In this framework, STRATUS leverages several different technical resources to provide an organisation with a layered, automated approach to help respond to distributed attacks by leveraging a suite of technologies to help counteract the impact and effects of distributed attacks (Burstein et al., 2012).

As illustrated in Figure 2.1, this technically adaptive approach is defined by the relationships between observations, failures or attacks indicated by the observation and the response required to address these threats in an automated manner.

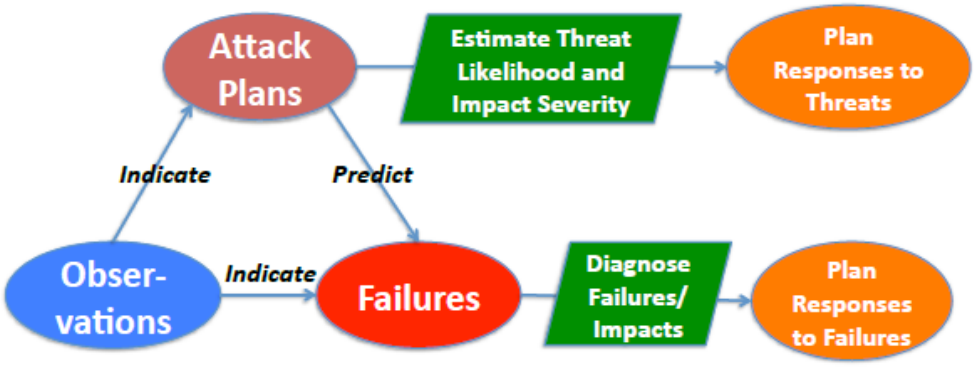

Figure 2.1: Response to observations in STRATUS model (Burstein et al., 2012)

Another technical framework is the Cyber Resiliency Engineering Framework proposed by Bodeau et.al (2011) in the MITRE technical report. This framework consists of three distinct disciplines namely resilience engineering, cyber security and mission assurance engineering. Resilience engineering focuses on establishing the goals for the phases of cyber resilience while cyber security is solely focused on addressing the threat actors and evolving or advanced cyber techniques. The mission assurance engineering ensures a focused approach to the overall framework. These three disciplines are depicted in Figure 2.2.

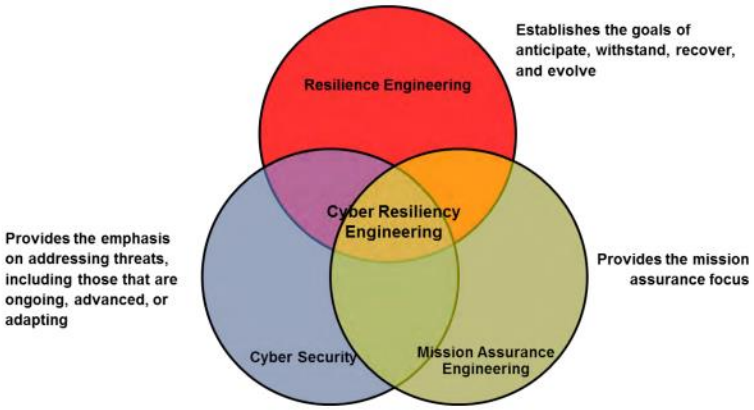

Figure 2.2: Key Sources for the Cyber Resiliency Engineering Framework

Using the three disciplines as a basis, the cyber resilience engineering framework align to the principles of Anticipate, Withstand, Recover and Evolve cyber resilience phases (Figure 2.3). These resiliency goals are supported by eight objectives which function together and provide the organisation a way to monitor the effectiveness of resiliency, through constant monitoring of the objectives and how these objectives can adapt to the evolving nature of cyber threats (Annarelli & Palombi, 2021; Jeimy & Cano, 2023)

As this framework adopts an engineering focus to define certain technical metrics, these metrics are able to evolve with the nature of the cyber threat identified. There are several supporting processes that are referenced within the cyber resiliency engineering framework which can be tailored according to the resources available to the organisation (Bodeau et al., 2011).

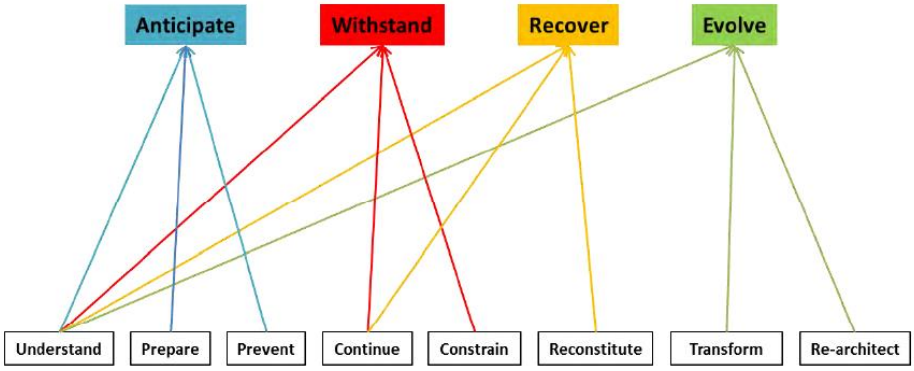

Figure 2.3: Cyber Resiliency Engineering Framework goals and objectives (Bodeau et al., 2011)

One of the most notable cyber resilience frameworks by Linkov et al. (2013) is the cyber resilience matrix framework leveraging off the resilience concept discussed in the cyber resilience definition section of this paper and adapting a previous resilience model which had been developed by Linkov (Linkov et al., 2013). These four phases, as shown in Table 2.3, consist of the plan/prepare, absorb, recover, and adapt phases. These phases are cooperatively associated in the matrix with the four domains of the cyber resilience organisational model which incorporate elements of physical, information, cognitive, and social factors (Linkov et al., 2013). The first of these four phases are usually centred around planning and co-ordinating the cyber resilience operationalisation process across the organisation. This phase usually consists of several risk assessments that provide the required impact assessments for the organisation to start building their cyber resilience capability from (Bagheri, Ridley & Williams, 2023).

This is followed by the absorb or withstand phase, in which the processes which support cyber resilience from both a technical and operating procedure is tested. The recovery phase involves recovering the systems to a state where they are available and operationally functional to continue with business activities. The final phase is termed the adapt phase and consists of a post incident review which reviews whether the cyber resilience operational model was successful in a real-life scenario or as part of a simulation. The feedback from this phase is used to determine whether a cyber resilience plan is still relevant and able to adapt to the evolving level of digital threats (Linkov et al., 2013).

Table 2.3: Four phase cyber resilience matrix framework (Linkov et al., 2013)

Category	Plan and prepare for	Absorb	Recover from	Adapt to
Physical	(1) Implement controls/sensors for critical assets [S22, M18, 20]	(1) Signal the compromise of assets or services [M18, 20]	(1) Investigate and repair malfunctioning controls or sensors [M17]	(1) Review asset and service configuration in response to recent event [M17]
	(2) Implement controls/sensors for critical services [M18, 20]	(2) Use redundant assets to continue service [M18, 20]	(2) Assess service/asset damage	(2) Phase out obsolete assets and introduce new assets [M17]
	(3) Assessment of network structure and interconnection to system components and to the environment	(3) Dedicate cyber resources to defend against attack [M16]	(3) Assess distance to functional recovery	(3) Assessment of network structure and interconnection to system components and to the environment
	(4) Redundancy of critical physical infrastructure			(4) Safely dispose of irreparable assets
	(5) Redundancy of data physically or logically separated from the network [M24]			
Information	(1) Categorize assets and services based on sensitivity or resilience requirements [S63]	(1) Observe sensors for critical services and assets [M22]	(1) Log events and sensors during event [M17, 22]	(1) Document incident's impact and cause [M17]
	(2) Documentation of certifications, qualifications and pedigree of critical hardware and/or software providers	(2) Effectively and efficiently transmit relevant data to responsible stakeholders/decision makers	(2) Review and compare systems before and after the event [M17]	(2) Document time between problem and discovery/discovery and recovery [S41]
	(3) Prepare plans for storage and containment of			(3) Anticipate future system states post-recovery

	classified or sensitive information			
	(4) Identify external system dependencies (i.e., Internet providers, electricity, water) [S31]			(4) Document point of entry (attack)
	(5) Identify internal system dependencies [S63]			
Cognitive	(1) Anticipate and plan for system states and events [M18]	(1) Use a decision-making protocol or aid to determine when event can be considered "contained"	(1) Review critical points of physical and information failure in order to make informed decisions [M17]	(1) Review management response and decision-making processes
	(2) Understand performance trade-offs of organizational goals	(2) The ability to evaluate performance impact to determine if mission can continue	(2) Establish decision-making protocols or aids to select recovery options	(2) Determine motive of event (attack)
	(3) Scenario-based cyber wargaming	(3) Focus effort on identified critical assets and services [M20]		
		(4) Utilize applicable plans for system state when available [M20]		
Social	(1) Identify and coordinate with external entities that may influence or be influenced by internal cyber attacks (establish point of contact)	(1) Locate and contact identified experts and resilience responsible personnel [S40]	(1) Follow resilience communications plan	(1) Evaluate employees' response to event in order to determine preparedness and communications effectiveness [S18, 19]

	(2) Educate/train employees about resilience and organization's resilience plan [M17, S29]	(2) Determine liability for the organization	(2) Assign employees to critical areas that were previously overlooked [S22]	(2) Stay informed about latest threats and state of the art protection methods/share with organization
	(3) Delegate all assets and services to particular employees [S15, 22]	(3) Stay informed about latest threats and state of the art protection methods/share with organization		
	(4) Prepare/establish resilience communications [S17			
	(5) Establish a cyber-aware culture			

The four organisational domains provide stakeholders with a guide on how to approach the operational aspects of each of the four phases of the cyber resilience matrix framework. As cyber resilience requires the input and support from diverse organisational disciplines, the organisational domains can also bridge gaps by promoting collaborative communication between stakeholders. Communication can be used as a means to foster ties between different stakeholders and promote collaboration between stakeholders in order to achieve objectives (Bunn, Azmi & Puentes, 2009).

Each of the frameworks mentioned in this section use a different naming convention for each phase but the fundamental purpose of each phase can still be linked back to the original NAS definition of resilience discussed in section 2.2.1. To ensure a uniformed approach to the naming conventions for each of the four phases throughout this paper, the researcher adopted the NAS wording for each resilience phase as the working definition for this paper. These phases are the plan, absorb, recover and adapt phases.

2.3 Summary of literature review

Stakeholders are participants who have a vested interest in the decisions made by an organisation and can effectively influence decisions which affect the overall goals of an organisation. Stakeholder influence can extend to both internal and external environments and as a result of this influence, stakeholders play a significant role in ensuring that an organisation derive value, from both a financial and organisational trust perspective.

When taking into account the proliferation and sophistication of cyber attacks being experienced by organisations on a daily basis, organisations have been forced to adapt their security control posture to ensure an effective approach to mitigating cyber risk. This includes complimenting existing, traditional security controls with a more robust and effective process.

As cyber resilience is a multi-disciplinary and interconnected process that brings together many different facets of an organisational structure, stakeholders play a significant role in ensuring that the overall objective of cyber resilience is understood and aligned across these facets of the structure. To enable and benefit from this alignment, it is imperative that stakeholders understand the phases of cyber resilience and how these phases form a holistic process in minimizing the impact of downtime caused by cyber events.

3. Theoretical Framework

This chapter discusses the theoretical framework selected for this study. This study uses the Cyber resilience matrix framework by Linkov as a lens to guide the study into the factors influencing operationalisation of cyber resilience within an organisation.

The Cyber resilience matrix framework is suitable for this study as the framework uses organisational domain metrics to measure impact across the four phases of cyber resilience within an organisation. As a case study was employed for this study, the organisational domains provide a guideline to formulate questions which can help answer the research question and objective of this study.

3.1 Cyber resilience matrix framework

There are several cyber resilience frameworks that have been proposed and highlighted in scholarly research which solely focus on the technical or operational aspect of the cyber resilience process. A few of these frameworks were briefly discussed in section 2.2.4 of chapter 2 and while both the technical and operational aspects are important facets of the cyber resilience process, organisational elements also need to be considered as business stability and continuity is most impacted by cyber threats (Estay et al., 2020).

Sabev (2020) noted that cyber resilience is a multi-faceted and multi-disciplinary concept and that the process to operationalise cyber resilience encompasses more than just the technical and operational aspects and that organisational and behavioural elements are crucial to the overall objective of cyber resilience. These organisational elements often have a bearing on the types of decisions that are made within an organisation and it becomes imperative for an organisation to ensure decisions are based on an adequate understanding of a concept such as cyber resilience.

Business stakeholders often do not understand concepts of cybersecurity as well as their IT counterparts, which leads to conflict as the business objectives and organisational cyber resilience do not align (Bagheri, Ridley & Williams, 2023). To address this issue, all stakeholders need to have a shared understanding of the cyber resilience process and how the process can support business objectives. There are a minimal number of studies that consider the organisational elements of cyber resilience (Bagheri, Ridley & Williams, 2023; Estay et al., 2020; Buchmann et al., 2020) and the impact it has on the cyber resilience operationalisation process. One of the most cited cyber resilience frameworks that include the organisational elements is the cyber resilience matrix framework by Linkov et al., (2013).

The Cyber resilience matrix framework proposed by Linkov et al., (2013), (Recall section 3.2.4 of Chapter 3) is an example of a cyber resilience framework. A study conducted by Bagheri, Ridley & Williams (2023) notes that the cyber resilience matrix framework can be used in different contextual settings and within literature a few examples included studies which investigate the resilience of smart water systems (Marchese et al., 2019), cascading threats facing critical infrastructure resilience (Wells et al., 2022) and population displacement due to disasters (Rand et al., 2019). What differentiates this cyber resilience framework from most of the other frameworks, is the addition of four distinct organisational domains namely the physical, information, cognitive and social which can be mapped to the four stages of cyber resilience which is plan, absorb, recover and adapt. The domains provide an organisational lens through which organisational metrics can be measured across the four phases of cyber resilience.

The four organisational domains draw its origins from the network-centric warfare doctrine that examine situational awareness across each of the organisational domains and how it informs the decision making process (Linkov et al., 2013). These metrics can be used to measure impacts across the four phases of cyber resilience and can be expanded upon to measure its implications across these phases of cyber resilience (Linkov et al., 2013). Through the incorporation of these organisational domains, the cyber resilience matrix framework provides an organisational level framework from which the phases of cyber resilience can be measured and managed and therefore provides suitable dimension for a case study where the main objective is to understand the effect of stakeholder perspective on cyber resilience operationalisation.

The physical domain references physical sources of information which deal with processes and identification of organisational performance, while the information domain relates to information most relevant to the physical domain which would include time required to complete initial evaluation and data usage development. The cognitive domain deals with the decision-making processes and implementation of the plans while the social domain reflects the organisational relationships required to ensure the successful operationalisation of cyber resilience culture (Uchendu et al., 2021; Bagheri, 2020). An example of the organisational domain metrics for each of the cyber resilience phases is shown in Table 3.1 with a brief description of each metric.

Table 3.1: Example of each metric of cyber resilience matrix framework (Bagheri, Ridley & Williams, 2023)

	Cyber Event Management Stages				
	Plan/prepare for		**Absorb**	**Recover from**	**Adapt to**
Organisational Domains	**Physical**	Maintain controls for cyber resources/create physical assets/evaluate systems interconnections	Use redundant services to continue operation/ reduce cyber threats	Resolve any system problem/assess cyber risk/evaluate recovery time/change irrecoverable items	Evaluate the system's configuration/ allocate new assets
	Information	Classify information resources/ prepare documents for IT suppliers/store valuable information/identify internal or external relationships	Identify the sensors/transfer information to relevant parties	Store log data for databases/ recover after an incident	Keep records of time taken between the incident, recovery and post-recovery solution
	Cognitive	Plan for cyber incidents/understand business objectives/organise cyberwar gaming	Apply a protocol for decision-making/evaluate achievements/id-entity important resources/develop appropriate policies	Identify any breakdown points/ make decisions during recovery	Review management response for a better decision/ discover the reasons behind the cyber attack
	Social	Communicate with external parties/provide training programs/delegate services to particular employees/improve resilience communication among employees/foster a culture of cyber resilience	Identify & communicate with cyber resilience professionals	Follow cyber resilience guidelines/determine responsible parties for cyber resilience	Evaluate employees' response to cyber incidents/allocate human resources/remain up-to-date about cyber risks

The cyber resilience matrix framework was used in a recent study by Bagheri, Ridley and Williams (2023) to understand the management perspectives of organisational cyber resilience in two different organisations. Through application of the organisational domains of the cyber resilience framework, the authors were able to provide results to substantiate their study.

The cyber resilience matrix framework is therefore a suitable framework which can be leveraged for this case study that focuses on stakeholder perspectives within an organisational setting and how these perspectives contribute to the factors influencing the different phases of cyber resilience. By combining the four phases of cyber resilience and the four organisational domains, the cyber resilience matrix framework will be used to enable the researcher to answer the research question and its associated objective.

4. Research Design

Research design is a comprehensive plan which focuses on the approach taken to fulfil the research objective and answering of the research questions. The research design includes the selection of an appropriate research method, sampling strategy and data collection and analysis approach (Bhattacherjee, 2012).

This chapter will address the research methods undertaken for this research. Section 4.1 introduces the research philosophy which presents both the ontological and epistemological choices for this research. Section 4.2 presents the research purpose, while section 4.3 presents the research approach to theory. Section 4.4 introduces the research strategy, while section 4.5 presents the data collection methods, encompassing the sampling technique and research instrument deployed during the research. Section 4.6 presents the data analysis methods while Section 4.7 presents the research quality. Section 4.8 provides the timeframe and section 4.9 discusses the ethics and confidentiality principles guiding this research. The chapter concludes with a summary of the research design in section 4.10.

4.1 Research philosophy

Research philosophy refers to the beliefs and assumptions of how knowledge is developed during a research process (Saunders, Lewis & Thornhill, 2019). There are two research philosophies that are discussed during this section, namely Ontology and Epistemology.

4.1.1 Ontology

Ontology refers to the assumptions made about the nature of reality and how we see the world (Bhattacherjee, 2012; Saunders, Lewis & Thornhill, 2019). The subjectivist view perceives reality made up of interactions with social actors and that the reality is socially constructed (Saunders, Lewis & Thornhill, 2019). From a subjectivist ontological stance, a phenomenon can be explained by the perspectives of the actors who are directly involved within a certain setting or reality and through these experiences, the researcher can understand and gain rich insight into those experiences (Wahyuni, 2012).

This main objective of this research focused on the stakeholder perspectives regarding factors influencing the operationalising of cyber resilience and therefore required an understanding of participants experiences through their interactions and participation. This notion is enforced in a book by Saunders, Lewis and Thornhill (2019) which emphasizes the requirement for a researcher to focus on the context and details of the situation to obtain the subjective meanings. To be able to explore these realities and obtain these meanings, this study followed a subjectivist approach.

4.1.2 Epistemology

Epistemology refers to what constitutes knowledge that would be deemed acceptable and valid (Saunders, Lewis & Thornhill, 2019). Since the study adopted a subjectivist point of view whereby reality is made up of interactions with participants, interpretivism assumes that participants experience different realities because of their lived experiences and provides insights on experiences from the point of view of the person experiencing them (Saunders, Lewis & Thornhill, 2019).

To enable the answering of the main research question, the researcher needed to form part of the social world of the participant and to enable that immersion in that reality, an interpretive epistemological belief was adopted by this research to allow the researcher to understand the point of view of a participant (Saunders, Lewis & Thornhill, 2019).

4.2 Research Purpose

Due to the nature of the research problem and questions to be answered, the study embraced an exploratory approach using qualitative data collected from interviews. An exploratory research approach is best suited when conducting research in new realms of inquiry, where the goal of the research is to better understand the scale of a particular phenomenon or behaviour (Bhattacherjee, 2012).

As the concept of cyber resilience operationalisation is still an emerging and fairly nascent topic, there is limited empirical research regarding the factors that influence cyber resilience operationalisation from a stakeholder perspective within the South African context and therefore, the exploratory approach was appropriate for the research.

4.3 Research Approach

There are several approaches to theory that involve the use of inductive and deductive methods. The deductive approach is usually employed for theory or hypothesis testing using empirical data and is sometimes referred to as theory testing method (Bhattacherjee, 2012). An inductive approach uses themes and patterns extracted from data to form a hypothesis about the phenomenon being researched and develop a theory as part of the approach (Bhattacherjee, 2012).

For this study, a deductive approach was used by the researcher. The deductive approach process begins with the testing of a theory, which can be proven to work or not within the research study or be used to construct more theories or expand existing theories (Bhattacherjee, 2012). As the researcher will be using empirical data from the case study to test the theory, a deductive approach is suitable. The researcher used the cyber resilience

matrix framework as a theoretical framework to guide this study and incorporated elements of the framework to shape the interview questions.

4.4 Research Strategy

The choice of a research strategy is guided by the research objectives and assists in answering the research question (Saunders, Lewis & Thornhill, 2019). A case study approach has several strengths over other alternate strategies such as surveys and experiments, by providing a richer, contextualised interpretation of the phenomenon based on the perspectives of multiple participants (Bhattacherjee, 2012). This strategy also allows a theory to either be tested or built according to data that emerges (Bhattacherjee, 2012). For this study, a single case study was used to provide the researcher with a strategy that could provide richer, contextualised data, gleaned from the views of the stakeholders.

4.4.1 Case Description

The organisation, referred to in this paper as Company A, is a medium-sized South African company based in the Western Cape and operating in the financial services sector. Company A has been in operation for more than 25 years and specialises in the financial services product domain, providing several different types of financial products to the market and forms part of a larger banking group. The use of the term, group, in the rest of this thesis is used to indicate the larger banking group who own Company A. Company A makes use of several customised built systems to perform its end-to-end business operations while leveraging several integration services, to enable the customer journey for both its web based online platform and internal customer service processes.

The organisational structure is made up of different functional departments, which provide specific centralised services which support the overall business objective of the organisation. These departments consist of specialised support services such as finance, marketing, IT, risk, legal, human capital and a number of customer focussed business operations and this organisational structure is reflected in figure 4.1 Company A also has several governance committees and risk forums that manage the overall risk and strategy of the organisation, which ensures that the business strategy is executed at various levels throughout the organisation.

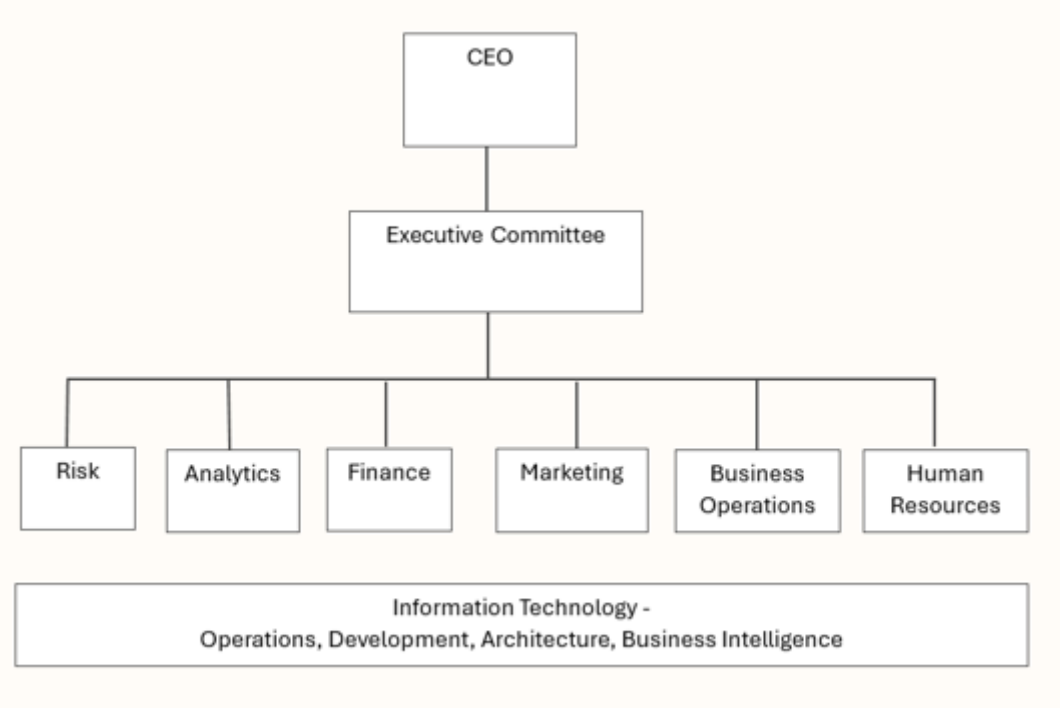

Figure 4.1: Organisational structure

The structure of these governance committees and forums allows a uniformed process to be followed and a funnel for raising important matters and escalations for internal and external risks, as well as a robust decision-making process to ensure risks are addressed and mitigated as part of the business operations.

These risk mitigation actions are operationalised through risk and impact assessments which provides a formalised way in which processes are amended and controls implemented, to manage the overall risk of the organisation and to stay within the defined risk appetite.

4.4.2 Resilience Management in Company A

To manage risks associated with adverse events such as disasters, an operational resilience team was established within Company A, which consists of designated individuals from each support area, who are responsible for ensuring the correct controls and processes are in place to mitigate specific resilience scenarios highlighted through risk assessments. One of these resilience risk scenarios include the cyber resilience operationalisation process which is a group directive to ensure there are controls in place to mitigate and recover from cyber threat events.

The group directive was formalised in the form of a guidance document which provides the organisation with a control framework, which can be tailored for the unique business requirements of the organisation. The document and its related standards were perused as part of the secondary data collection process and provided the researcher with an overarching guide of the operationalisation process in place at the organisation.

4.5 Data Collection

Through the collection of several sources of data, the case study benefited from the richness and variety of data which conformed to the rigour required for qualitative studies (Forero et al., 2018). The following data collection techniques were used for the study.

4.5.1 Research Instruments

The study used semi-structured interviews for data collection. The questions in the interview guide were open ended and used as the primary source of data. These questions were drafted based on the cyber resilience matrix framework, which provided the researcher the organisational domains concepts and related metric examples which was used as a guide to draft questions which could measure impact across all four phases of cyber resilience. This process ensured that the interview questions were linked to the research question and that the questions were structured in a way to ensure conversation which provided the required information (Castillo-Montoya, 2016). The use of open-ended questions also provided the researcher the opportunity to ask follow up questions based on the answers provided by the participants and thus enhanced the richness of the information provided by the participants.

To complement the interview data, relevant documents were used as secondary sources of data to enhance the richness of the data (Elo et al., 2014; Saunders, Lewis & Thornhill, 2019). While the researcher was provided access to documentation, the documents were highly confidential in nature and as part of the risk assessment performed by the organisation for the approval to conduct the research, the researcher was only allowed to incorporate high-level notes from the documentation. Despite the limited use of documentation for the research, the combination of these data sources benefited the case study as the collection of primary and secondary data provided greater detail and insight (Bhattacherjee, 2012).

4.5.2 Sampling

Sampling is defined as a statistical process used to select a subset of a population for the purpose of making observations about that population. The first step in sampling comprises the selection of the target population (Bhattacherjee, 2012). In this study, the target population was the financial services organisation used for the case study. The second step entailed selecting a sampling frame. There were 12 participants who agreed and consented to the interview process and are represented in Table 4.1. These 12 participants form part of the resilience team with representation from different organisational departments, with a diverse set of qualifications, cultural background, experience and skills.

These participants were chosen by the executive structure of Company A to ensure suitable representation from all the relevant departments and for awareness purposes so that the concept of cyber resilience was understood and managed by these stakeholders and their respective teams within the organisation.

Purposeful sampling was used select the participants as these participants could provide the rich insights required for the research (Saunders, Lewis & Thornhill, 2019). As the 12 participants already formed part of an existing structure responsible for cyber resilience within the organisation, the sampling was also convenient.

Table 4.1: List of interview participants

Participant ID	**Role**	**Gender**
Participant A	Information security practitioner	Male
Participant B	Technical specialist	Male
Participant C	Technical release specialist	Male
Participant D	System owner	Male
Participant E	Legal specialist	Male
Participant F	Business operations manager	Female
Participant G	IT Risk manager	Male
Participant H	Business Risk manager	Male
Participant I	Senior IT Executive	Male
Participant J	Technology Head	Male
Participant K	Finance manager	Female
Participant L	Business solutions architect	Male

4.6 Data Analysis

The data collected during the study was analysed through thematic analysis. Thematic analysis has been widely cited as a comprehensive method to perform qualitative analysis and a suitable method to analyse themes extracted from interview data (Braun & Clarke, 2006). The researcher applied the six phases of thematic analysis recommended by Braun and Clarke (2006) for the thematic analysis of the interview data and these phases are presented in table 4.2.

The researcher made use of the Microsoft Teams application for its recording and transcription feature during the interviews. Once the transcriptions were available, the researcher analysed the transcripts and manually extracted the codes for each phase of the cyber resilience matrix framework. These codes were collated and used to develop themes which emerged from the interview data and which supported the overall objective of the study (Bhattacherjee, 2012) and have been included in Annexure E.

Table 4.2: Braun and Clarke six phases of thematic analysis (Braun & Clarke, 2006)

Phase	**Description of the process**
Familiarizing yourself with your data	Transcribing data (if necessary), reading and re-reading the data, noting down initial ideas.
Generating initial codes	Coding interesting features of the data in a systematic fashion across the entire data set, collating data relevant to each code.
Searching for themes	Collating codes into potential themes, gathering all data relevant to each potential theme.
Reviewing themes	Checking if the themes work in relation to the coded extracts (Level 1) and the entire data set (Level 2), generating a thematic 'map' of the analysis.
Defining and naming themes	Ongoing analysis to refine the specifics of each theme, and the overall story the analysis tells, generating clear definitions and names for each theme.
Producing the report	The final opportunity for analysis. Selection of vivid, compelling extract examples, final analysis of selected extracts, relating back of the analysis to the research question and literature, producing a scholarly report of the analysis.

4.7 Research validity and reliability

Quality of qualitative studies are often measured by the validity and reliability of the data (Golafshani, 2003). The reliability and validity of the data is essential for the accuracy and reliability of the research (Golafshani, 2003).

4.7.1 Research validity

In the qualitative study process, both internal and external validity constructs are relevant to the credibility and accuracy of the data (Patton, 2014). Internal validity relates to the checks that ensure data accuracy, while external validity focuses on generalisation from the data in question (Patton, 2014). For internal validity, the interview notes and transcripts were shared with participants to ensure that all transcripts were captured correctly and accurately. Credibility was further supported using quotations, to highlight the applicability of the themes that emerged from the data. External validity was achieved by documenting the entire process that was followed for this study.

4.7.2 Research reliability

Reliability is assessed by the accuracy of the findings and the consistency of the results which can be measured over time (Golafshani, 2003). One way in which reliability can be measured, is through the application of data triangulation. Data triangulation uses multiple research instruments to ensure the findings are accurate (Golafshani, 2003). For this research, data triangulation was applied through the collection of data from a primary and secondary source of information. The use of a secondary data set assisted in the validation of the interview data provided by the participants.

4.8 Timeframe

A cross-sectional timeframe was used for this research as the research focussed on the organisation at a point in time (Saunders, Lewis & Thornhill, 2019). The choice of a cross-sectional timeframe approach was further influenced by the time limitations of the Master's degree programme which must be completed within two years.

4.9 Ethics and Confidentiality

Ethics and confidentiality are a crucial part of the overall governance process during the research process. Before any data was collected as part of this research, ethics approval was obtained through the ethical approval process at the university. Once ethical approval had been provided by the university, the researcher completed a risk assessment at the organisation being used as a case study, to ensure the researcher complied with the organisation's privacy and confidentiality policies.

Once the risk assessment was concluded and the research was approved by the organisation, the identified participants signed consent forms and were informed that their participation in the research was voluntary and that they were allowed to withdraw their consent at any point in time. All participants' details were kept anonymous and confidential, to ensure adherence to privacy legislation and conditions of both university and organisation approvals.

While the researcher was given access to secondary data as part of the research process, no specific details contained in any of the secondary data, in the form of policies or standards, was included in the research findings. Any reference to the secondary data was kept to a minimum based on the conditions of the approval by the organisation.

The researcher also clarified the research to all participants before the interview, so that they could understand the research they were taking part in, as well as the questions that would be asked in the interview. During the entire data collection and analysis process, least privilege principles were applied to restrict access to the collected data and the transcripts of the data was also always encrypted.

4.10 Summary

This chapter presents a summary of the research design that was used for this study. Table 4.3 summarises the research methods.

Table 4.3: Summary of research design

Ontology	Subjectivism
Epistemology	Interpretivism
Approach	Deductive
Strategy	Case study
Purpose	Explanatory
Timeframe	Cross-sectional
Data Collection	Semi-structured interviews and document analysis
Data Analysis	Thematic analysis

5. Research findings

The main objective of this research was to understand the factors that influence how cyber resilience is operationalised within organisations. This chapter introduces and explains the outcome of this study and attempts to answer the main research question "What factors influence how cyber resilience is operationalised within organisations?".

The findings are presented and discussed based on the cyber resilience framework matrix introduced in Chapter 3. Section 5.1 to 5.4 presents and discusses the findings of the interviews and is arranged according to the four phases of the cyber resilience framework matrix in order of plan, absorb, recover and adapt. A summary of the factors influencing each phase of cyber resilience is presented in table 5.1. The section concludes with a summary of the chapter in section 5.5.

Table 5.1: Factors that influence each phase of cyber resilience

Cyber resilience phase	Factors influencing operationalisation
Plan phase	Risk appetite
	Business requirements
Absorb phase	Importance of data protection
	Adequacy of testing system resilience
Recover phase	Impact of recovery time on business operations
	Value of data quality as part of recovery phase
Adapt phase	Emerging technology trends – Impact of AI
	The need for more training and awareness amongst staff
	Learning from the post incident review process

5.1 Factors that influence the plan phase

The findings from the study indicate two factors that influence the plan phase of cyber resilience operationalisation within Company A. The plan phase is the basis from which an organisation prioritises the resources required to effectively build a cyber resilience plan. The following section presents how risk appetite and business requirements influences the organisational priorities and resource requirements during the plan phase of cyber resilience operationalisation.

5.1.1 Risk appetite determines organisational priorities

The risk appetite theme was consistent with cyber resilience dimensions examined in several studies which focus on the contextual organisational dimensions of risk and governance that influence cyber resilience implementation (Tsen, Ko & Slapnicar, 2022; Carías et al., 2020; Pavão et al., 2023).

Risk appetite, which defines the amount of risks an organisation is willing to take to meet their business objectives (Board, 2013), was a central factor that the participants highlighted as being important at the planning phase of cyber resilience. The participants in this study felt that the organisation's risk appetite influenced important decisions in relation to cyber resilience. Participant H highlighted how risk appetite influenced the risk management practices implemented by Company A which consisted of high, medium and low risk categories with various controls associated with each type of risk category. If the risk appetite shifted between the levels of high and low, the associated controls would be adjusted to ensure the required level of controls were in place to mitigate the risk.

The risk appetite also had an impact on organisational priorities including resource allocation. For example, Participant H stated that: "*from a prioritization point of view, looking at the level of risk and the impact of those risks...the higher the impact and severity of that impact, the higher priority*". Participant G, an IT risk member, echoed similar sentiments and emphasised that from an IT risk perspective, risk appetite would determine the way certain technical processes were prioritised within the business. "...*if what we're trying to achieve is technically either impossible, extremely challenging or the cost is not beneficial to what we're trying to achieve, then I think that would drive one to maybe reassess how we're prioritizing*".

For Participant D, the organisation's risk appetite played a pivotal role in his decision making regarding the amount of effort required in implementing technical safeguards to prevent system downtime. In his specific case, he stated that certain services for customers would be prioritised over having the entire system functionality available. "*If the business isn't willing to run up the bill to invest in a high availability situation... it's your risk appetite for the business and the business makes that decision*."

Participant C further explained that if there was a change in risk appetite, it would directly influence the way he would complement or amend existing operating procedures. Participant C ventured that he would always take direction from the business risk appetite as through his number of years of being employed by Company A, he had seen many changes in the risk profile of the company and the accompanying risk appetite. "*What is the company's risk appetite versus what they're trying to achieve? So, there's always a balance, especially in*

business in terms of how much can you risk versus what is the impact of when that particular risk eventually materializes".

Risk appetite informs the **policies and standards**. Policies and standards serve as a guideline from which controls and processes regarding risk management could be tailored to support organisational objectives which in the case of cyber resilience would be the objective of continuous business operations. Several participants cited changes in group policies and standards as factors that would influence decision making during the planning phase.

Participant A stated that a change in policy or standard, would directly influence the way certain controls would be configured within the cyber resilience process and therefore change his approach to a risk scenario. "*Depending on the circumstances, what influences change in priorities is dependent on the factors that come into play*".

These changes would require additional resources or investment, which the business would need to cater for and was therefore always a consideration when it came to technical planning. These types of planning and practices have been linked to the theme of governance within cyber security and highlighted as way to prepare leaders and stakeholders for managing cyber security-based programmes (Stine et al., 2020; Loonam et al., 2020; Dupont, 2019)

"*Policies and processes that have been signed off and implemented*" (Participant E) was essential in ensuring uniformity in terms of approach to implementing processes that provide a baseline cyber control environment, while ensuring a level of understanding amongst all stakeholders. When asked what would influence a change in priority from a planning perspective, Participant E stated, "*I think it would be business driven and if it's something that aligns to the strategy, I think it's important that that we as a support function remain flexible".* From an operational risk perspective, participant H stated that a change in policy or standard, would require a shift in priority as it may impact the status of a risk assessment and affect the outcome of the additional controls and reporting required. This would have a direct impact on how the risks are effectively mitigated.

5.1.2 Business requirements inform cyber resilience resource requirements

Several participants referenced that the business requirement would dictate which resource support requirements would be needed from their department and if the business requirement changed, it would have a direct impact on the level of support. The business requirements for an organisation are based on the business objective and gives senior executives a view to execute and deliver on the strategic deliverables for the organisation, such as risk initiatives like cyber resilience (Loonam et al., 2020).

Resource requirements is often referenced as an important part of any organisational resilience discussion, as resources are allocated from various, diverse stakeholders with different interests, which can lead to conflicting objectives (Haki, Aier & Winter, 2016).

An example of resource considerations was provided by Participant E, who stated that cyber risks were difficult to prepare for and if the business requirement for a certain risk had evolved from a simple attack to a more comprehensive and sophisticated attack, the flexibility to adapt to the change in business requirement change would require additional resourcing:

"*So, it's just to find that balance between what we know as a risk from, you know, our discussions with business and from a strategy perspective versus that which we can't foresee*" (Participant E).

Several other participants had similar views about how the business requirement would influence their decision to change resources supporting certain work items as part of the operationalisation process but that if the intended outcome remained the same, they were comfortable to adjust their resourcing schedules. *"If we look at this, I think the first thing we'll need to do is to, from a planning perspective is understand what the business requirements are, what is it we actually want to achieve?",* said Participant G*.*

Participant H shared that when a business requirement changes, it was important to re-engage all stakeholders involved in the process, to ensure that the change did not have unintended consequences such as creating conflict about whether the change required additional resources. This was important to discuss so that all stakeholders were on the same page, "*So that we fully understand the requirements within the organisation"*.

From an executive management perspective, participant J shared similar views as some of the other participants about how a change in business requirement or direction, would impact the number of resources allocated towards cyber resilience, as well as the amount of effort needed to upskill to understand evolving threats, "*If the group goes a different way in terms of technology, making sure that your people are upskilling in that tech is important and that you get involved early on in that process*". Participant J further elaborated that a change in business requirement was sometimes necessitated by events outside of the organisation control, such as macro or microeconomic event. "…*that would also be the if the business priorities changes, then obviously we change according to that and that can obviously be triggered by a macroeconomic event with the saying OK, let's change our approach".* Such changes in approach would have a direct impact in the resources required from both a cost and skill perspective.

5.2 Factors that influence the absorb phase

The absorb phase utilises the contextualised outputs of the planning processes, to technically prepare for the identified cyber risks. Information integrity is central to the absorb phase (Recall Chapter 2.2). Our participants cited data protection mechanisms as well as testing processes as being important determinants of information/data integrity within Company A and as being critical aspects of decision-making during a cyber incident.

5.2.1 Importance of data protection

When asked about what informs their decision when it comes to mitigating risk as part of the cyber resilience operationalisation, data protection was mentioned several times during interviews with stakeholders as an important consideration.

For Company A specifically, data protection was perceived to be important to its operations because of the regulatory and compliance obligations. These regulatory policies require the organisation to securely store several different data fields of a customer for a required amount of time. Insights garnered through the process of data analytics, also provided the organisation with rich information which was used for marketing and financial decisions (Participant J). In respect of data protection, the participants raised two main aspects namely data access and data availability.

The importance of Data access

Restricting data access is one of the fundamental steps an organisation can take to minimise the risk of data exposure and is aligned to the availability aspect of information security (Stamp, 2011; Bagheri, Ridley & Williams, 2023). Data access is also referenced as a required security safeguard for data protection, as part of the Protection of Personal Information Act (POPIA), to ensure no unlawful access to personal data (Adams et al., 2021) Participant J addressed data access as an important aspect of data protection and an important part of his role within Company A. If there was a change in data classification requirements, it would require an adjustment of access on a user and system level, to minimize the amount of data risk within that system. Participant J stated that "*If there's no procedures in place for applying and granting access then it becomes a nightmare to all".* An example of such a change in requirement was described by participant J.

> *"Especially when it comes to data and databases is access that if you've got any controlled use users or user groups rather then you know if there's a breach or whatever case, maybe it's much easier to isolate that, much easier to revoke access to certain groups if you aren't sure."* (Participant J)

A few participants also highlighted data access from a third-party connection perspective and stated that both internal and external data access needed to be monitored as part of cyber resilience operationalisation. Participant A stated that he worked directly with third party connections and "*would check that the connections to the business is secure as well as any data storage shared outward is obviously as well secured, so that would be an influence in my mind".*

This view was also shared by Participant H who reiterated the need to monitor access on all systems that are bounded by the organisational design "*so that's basically all systems that we worked with within the business those are the systems that we need to ensure are catered for and external systems that we may be using as well".*

Similar challenges associated with data have been highlighted in literature and is consistent with the challenges of handling data during an incident (Hausken, 2020), as well as the implementation measures required to ensure data security (Petrenko, 2022). Participant D also briefly spoke about the POPIA regulation which governs the protection of personal information in South Africa and stated that strict access to data was a requirement to ensure adherence to some of the data privacy principles and prioritised that as a key part of his operational duties.

Data availability and its importance in cyber resilience

Various participants also spoke about data availability as being another important aspect of decision making. Participant K, whose role involved ensuring data was accurate for both financial reporting and regulatory purposes, indicated that having data readily available during the absorb phase was critical to her role. She felt that if business was unable to quantify real time losses during a cyber event due to data availability, it could lead to an understating of losses and have consequences for the organisation.

Participant B also touched on the positive advantages of having data availability even though the organisation had been impacted by a cyber event. In his opinion, the reputational advantages for the organisation would be positive with a higher level of trust with the customer. For participant B, this was an important consequence of his responsibility in cyber resilience operationalisation, even if his role was more technically focused.

The availability of customer data was highlighted by participant D and E, as Company A stored many types of personal information in respect of the customer. Participant E questioned whether the organisation could protect all data stored across all systems, if the resilience test for data availability was not adequate.

> *"So obviously, if the resilience isn't tested to that, let's say that extreme to ensure that we can keep every record safe and then that becomes the area in which our concerns are raised from experience, it always only takes 1 customer to really you know have a really negative experience when it comes to data for you know red flags to come up*." (Participant E)

Participant D echoed this sentiment by stating that his concerns would be the impact on the reputation of the company, specifically "*reputational damage in the event of customers getting the data out there"*, especially if after a cyber event had occurred and the customer data was unavailable due to a system outage. Company A would then be unable to confidently confirm that no customer data had been leaked during a cyber event. This unavailability of data may lead to irreparable damage to the organisation as it would impact customer trust (Dupont, 2019).

5.2.2 Adequacy of testing system resilience

Testing system resilience, which refers to the method taken to test that the functionality of the system behaves in the correct manner during an adverse event, was perceived by several participants as an important aspect of the absorb phase. Testing the business system for resiliency forms the core part of cyber resilience as it provides operational evidence that the system is robust enough to withstand the effect of a cyberattack (Petrenko, 2022; Linkov & Kott, 2019; Annarelli, Nonino & Palombi, 2020).

Selecting correct systems. Participant A stressed the importance of the correct systems being selected and tested, as that would be a key driver in his decision making regarding the control testing for each system. Failure to properly test the correct systems could mean a successful cyber breach impacts other units across the organisation "*I've mentioned that the group would be exposed, so failed system test in organisation would mean exposure to not just our branch but our group as well, which is catastrophic*." - Participant A. These types of breaches can have significant impact on organisations, especially those nested in the financial industry who store significant amounts of customer and transactional data (Dupont, 2019).

Participant G stated that the purpose of the absorb phase was to ensure that: (a) the correct systems were selected for testing and (b) the type of testing performed was adequate and relevant and that if system testing was not performed at the required level, it would expose the organisation to both reputational and regulatory risk and that would impact his level of comfort with the testing methodology. From this perspective, Participant G would relook at the testing scenario as well as the frequency to ensure that "*There should be some sort of policy that says that it needs to be tested on X amount of days in a 12-month period".*

Adequate testing. In addition to testing the right systems, Participant G emphasised that ensuring the correct type of testing was selected for the targeted systems was equally important as it would impact the operationalisation process. The impact of not using the correct type of testing steps would require a change in resourcing, priority and even test plan to ensure the adequacy of the test result. The impact would also be felt by business as there may not be a full understanding of the different types of testing methodologies and its requirements for a successful test.

"We need to understand the criteria of that and also, and if we're not doing a full test, what do we actually get out of it and the business needs to understand the criteria." (Participant G)

Participants H and I had similar views about the impact of ineffective or outdated testing plans. Participant H stated that it was important to "*ensure that the systems are tested for the most recent or relevant threats against level of security"* and that if that type of testing was not that there may be consequences "s*o if we don't stay ahead of the curve, the chances of us being able to mitigate or counter that maybe limited".*

Participant I discussed some technical aspects of certain processes that are critical to the function of the business and how each process could potentially be an area of compromise. It was therefore important to Participant I that test cases and potential scenarios were drawn up by experienced individuals who could also provide priority so that in the event of a real attack occurring, that they could make swift decisions about whether a service was a priority or that it "*might be a P2 we can recover that in a later stage"*.

Participant I further stated that priority in this case was a very crucial deciding factor for him as he would have to take responsibility for allocation of resources and that allocating resources to the incorrect testing methodology, would have a detrimental impact on the business.

> *"I guess from a dev perspective, what concerns me is I guess if that we miss something that's going to policies, but also that we not up to date with the latest couldn't fix the threats that are on the horizon and not future threats potentially*." (Participant I)

5.3 Factors that influence the recovery phase

The recovery phase refers to the point at which a system has adequately recovered to a working state. Two main findings emerged as being important for the recovery phase: the impact of the recovery time to the overall functioning of business and the value of data quality. The impact of recovery time was considered crucial to the overall successful outcome of cyber resilience, as it provided a measurement of the time it took the business to be operational, while the value of data quality was highlighted as important to ensure accurate and correct data was processed after the events of a cyber-attack.

5.3.1 Impact of recovery time on business operations

Recovery time is essential to the overall success of ensuring business continuity and is the cornerstone of the cyber resilience operationalisation process (Linkov et al., 2013). When asked about what they felt was crucial to recovery, the participants highlighted data recovery and speed of recovery as two separate but interdependent factors.

The importance of data recovery. Several participants focused on the impact of the customer and the loss of data as their primary concern when it came to the impact of a longer recovery time. From a data loss perspective, participant L perspective was shaped by his intricate knowledge of the various services that support the business-critical system functionality and was concerned that system downtime had "*some financial implications*" and that depending on severity of issue, data loss could equate to losing some critical information, "*you know, financial transactions, you don't want to lose those*". He also added that "…*from a customer point of view, you know if your system's down, you lose trust, you know, so they probably could look for another one of your competitors*. *So yeah, you don't wanna lose your customers*". Participant L would change approach in system designs to ensure that any impact on either the loss of data or customer experience, was kept to a bare minimum to ensure "*zero loss of data so and least minimal downtime for affected users".*

Speed of recovery*.* A few participants highlighted the technical recovery time as a key factor in their risk management strategies to ensure that the business expectation regarding the amount of time it would take systems to recover, was both realistic and feasible. The operational recovery can be implemented as a framework on its own due to the various tendencies which support the recovery time objectives (Onwubiko, 2020). Participant G perceived his role as "*sitting in between IT and business*" and that the function acted as a *"kind of a broker between the two because business can have certain views. IT will have certain views and we try and need to make those views come together because business may be unrealistic and so they want something up in 30 minutes and it's just not achievable*. Participant G stated that the impact of downtime had to be socialised with stakeholders across

the business to "*drive some sort of consensus and alignment of views as to what is, umm, actually acceptable as to what would be an operational loss from a business perspective."*

From a technical perspective, both Participant B and C focused on the speed of the recovery time as the main objective of cyber resilience was to ensure that systems were operationally available and functional for staff members. Participant C said that his role within cyber resilience process focused on the "*speed of recovery and effectiveness of the recovery*" to ensure that all support teams worked towards the goal of ensuring systems were operational within the agreed time.

> *"Ideally you would want your business to flow and to just grow from strength to strength, but obviously we have these obstacles that arise and the important things is obviously once something's identified and acknowledged as an issue, it's how quickly you can bypass that or overcome that and get business to that state again, that it's flowing again."* (Participant C).

Participant B felt that due to the technical nature of his role, he and his team had a much better understanding how difficult it was to ensure an effective recovery since "*we would actually test the resilience of your environments and system*". It was important to Participant B that any recovery process and subsequent testing of systems was pivotal in providing assurance to fellow stakeholders and staff that the technical process was effective enough to prevent any delay in ensuring daily work activities could continue. Subsequently, any downtime impact that was not adequately catered for from a technical perspective would negatively impact his involvement as what he does was measured by "*How fast you can get it fully functional and back up and running so that the impact and downtime is minimal."*

5.3.2 Value of data integrity as part of recovery phase

A few participants highlighted how the value of data quality played an important role, as the accuracy and completeness of data was important for analysis and reporting tasks. Data corruption is a risk that is associated with restoration and is therefore important to ensure the recovery is done in the correct order to avoid data issues (Onwubiko, 2020). Without the validation of the data being accurate and complete, certain processes would provide inconsistent or incorrect variables and information (Colicchia, Creazza & Menachof, 2019).

In respect of Company A, these incorrect variables would result in data quality issues and impact across the business operations in the form of marketing communication being sent to wrong customers, consent problems or affecting data decision making processes.

The impact of data quality in an operational setting was highlighted by participant K as of high importance due to the significant value it represented to the organisation. Data quality within the recovery phase would be checked in way such as to "*perform a task that I did maybe*

before the attack happened to see if I'm getting this the same results". This was also a process to ensure that no data had been affected as part of any cyber-attack as the reliance of correct data was based on the fact that in participant K operational role "*the department is driven by data".* According to participant K, If the results of a test performed before an attack or simulation was different from after the recovery of a system, it could lead to data quality issues and inaccurate reporting of financial and customer information which in turn could lead to regulatory issues and high-risk audit findings.

> *"Being able to prove that you know my information after this event is valid and accurate and complete, this is quite a difficult process that the team has to focus on because if cyber-attack happens in any company that becomes like a high audit risk."* (Participant K)

Having been employed at Company A for several years, Participant J stated that the importance and value of data had grown over the years he had been employed at the organisation and that data had transformed from being purely used as reporting numbers into a decision-making tool that could provide many competitive advantages for Company A. Due to the importance of data, the operational focus during recovery would be on data quality and ensuring that the data output is repeatable and accurate as stated *"I think that's the most value I would get out of knowing why and how data is impacted".*

The quality of the log data, in terms of completeness and accuracy, was mentioned by participant A as important as the logs were sources of data for investigative purposes. Another set of logs would also provide data to confirm whether the controls that had been implemented, was effective enough to provide assurance regarding the quality of the data. "*We have alerting and monitoring in place for this and we will obviously was with us for me to determine if this is a success or not."* If the data quality of the logs was not accurate, participant A stated that he would need to implement another set of logs to adjust settings as "*These are important facts to me because we need to ensure that it's either it happened or what has been exposed*."

Participant I also referred to the importance of telemetry data to measure how hardened a system was against an adverse event. In respect of the system development cycle, participant I further stated that the logs provided insights into whether the system booted in the correct manner and whether the staff was able to log on and perform functions to enable continuous business delivery.

5.4 Factors that influence the adapt phase

The adapt phase is used as a process wherein an organisation can adapt, amend or even redefine cyber resilience processes to ensure it can withstand the ever-evolving nature of cyber threats.

Artificial intelligence (AI), training and awareness and post incident review feedback were aspects that stakeholders deemed as important factors to the overall maturing of the cyber resilience process within the organisation.

5.4.1 Emerging technology trends - The potential impact of AI

The rapid emergence of AI was highlighted by several participants as a topic that would influence their thinking in respect of how to prepare and approach certain operational processes post an incident or part of the adapt phase in future. The participant perspectives regarding AI comprised of two main themes: AI as a potential threat and AI as a useful tool for automating manual processes which could improve efficiency.

The potential threat of AI. Participant A emphasised the threat of artificial intelligence and the ease in which controls could be exploited through using the advanced reasoning capabilities of artificial intelligence and merely using the prompt platform to provide answers to assist with how to circumvent security controls such as how "*people can ask AI to how to do hack stuff now."* Participant A further elaborated that while it was a challenge to ensure business understood the security risks surrounding the current system environment, artificial intelligence would add another layer of complexity and would require him to adjust his approach to communicating this threat to business but also to understand how artificial intelligence would complicate efforts to secure the technical environment against scenarios that may not have been adequately catered for by traditional risk assessment processes.

He also felt that artificial intelligence could develop into a source of threat intelligence that could aid the resilience effort "*because the world's always changing, there is new things being released into the wild continuously*" and that this was an opportunity to enhance the way that he would prepare for cyber resilience and therefore provide continuous improvement. Automation and use of autonomous agents could significantly improve response times and scale but also introduce other risks (Ligo, Kott & Linkov, 2021)

This perspective was further supported by Participant I who felt that with the rise of the ChatGPT, a free artificial intelligence platform, direct access to more complex technical information was much easier for threat actors and that these threat actors could have no experience in performing cyber threats but could easily grasp certain techniques through asking ChatGPT questions such as "*how do I use Wireshark to read packets?".* He also felt that with AI, more people would be able to learn how to practically perform threats with minimal knowledge.

> *"Think of what people can achieve with very little knowledge at the moment. What can happen with the all the devices that they have and what's happening in the world with the speed of things like AI?"*

AI as a useful tool. While participants A and I spoke about the potential dangers of AI to cyber resilience, Participant B felt that AI could have a big impact in the way technical operationalisation processes were mapped and tested as part of his technical responsibilities. He believed that AI could be utilised to cut down on unnecessary technical health checks and provide a more robust view of the technical enterprise landscape and its related vulnerabilities and blind spots.

From a business operations and risk perspective, AI was perceived as both an enabler for ensuring that updated and more efficient use cases could be tested as part of risk assessments within the business environments but also referred to as a "*wildcard*" as the impact it could have on cyber resilience as a whole was unknown to Company A according to participant H. Participant F stated that he would have to learn about AI and the impact it can have on the current way of thinking as his perspective was that without improving his own knowledge about the topic, it could potentially be a risk as "*with technology moving so fast…, one has to stay relevant and need to be knowledgeable about it, not just in your silo of what's happening in your current organisation, but across other organisations as well"*.

Conversely, participant K felt that AI could provide the organisation with an opportunity to improve certain areas of overall cyber resilience and to assist with a faster way to test systems as part of the recovery process during real time events. Participant K applied this to her own department and stated that the manner in which they could more efficiently complete data checks to ensure completeness post a cyber event, would be very advantageous.

"*I think AI would speed up the process of being able to pull out information before a cyber-attack and information after, you know, be able to quickly summarize that information*. *You know, to give me meaningful insights. I mean you facing a cyber-attack if I could you know help improve you know, speed up the process of how we doing things I think it could be seen as a positive yeah."* (Participant K)

A similar school of thought was held by Participant L, who felt that AI could be used in a constructive manner to assist the organisation with automating the threat discovery process which is used within the risk assessment process "*so in a positive way, we would be able to use AI to scan our environment, identify the threats".*

5.4.2 The need for more training and awareness among staff

Training and awareness were also perceived as an aspect that stakeholders felt were crucial for the continued development of the cyber resilience operationalisation process. Training has been cited as critical to the overall ecosystem of preventative cybersecurity measures (Fischer-Hübner et al., 2021; Carías et al., 2020). During the interview process, most participants mentioned training and awareness as an area that required focus within the organisation. While the organisational resilience team was responsible for the overall operationalisation of cyber resilience across business, there was a general feeling that all staff should be trained and informed about the cyber resilience process.

Raising awareness is noted as a proactive form of communication which can help bridge the divide in understanding about the reality of cyber threats between business and IT (Dupont et al., 2023; Hausken, 2020). If the business was more aware of the type of cyber threats that were prevalent within the industry, there would be better understanding regarding the importance of cyber resilience and more commitment from business in terms of both resource and finance allocation (Participant, B, C, G and D).

Participant C's perspective was that the current set of cybersecurity awareness training was generic and completed as a 'tick box' exercise, instead of being contextualised to the individual or staff member department. This was an area that he believed needed a more pragmatic approach, combining training material with verified real world cases and the fallout of breaches at organisations.

> *"My problem with it is that I think it gets done by the people doing it on a get it done basis. I'm just quickly gonna get it done and just quickly click through it and there we go. As opposed to a robust knowledge share on that and what I deem to call it little penny drop method you know so this one someone understands something they will be more suited to acting to it*." (Participant C)

The lack of awareness was one of the reasons that certain types of scenario testing was not completed as part of the risk assessments (Participant D). He explained that departments would rather stick to the "*tried and tested* [*scenario testing methods]. I don't think business is fully aware of the threats there are and the impact it might have and that's probably why we don't have a full checklist of all the scenarios.*".

Awareness was also an important consideration for both participants I and J, as they both believed that awareness was the foundation for an impactful and more successful training programme. According to Participant I, it was the collective responsibility of the staff to understand the nature of threats that could disrupt business operations and help contribute operationally towards the success of cyber resilience.

> "*it's actually everybody's responsibility to understand what is the impact that decisions that make when they come to technology and that is from a private life from a when you go to work, the things you wanna install it's when you look at why someone says no to something they're not doing it because they want to annoy you or they think you not working hard enough. They are valid security concerns and I think maybe that's something that needs to land*" (Participant I)

Participant K stated that before she had formed part of the operationalisation process, she did not understand the structures that protect the critical systems and infrastructure of the organisation. Participant K felt it important to "*being able to bridge that gap, knowledge gap"* and that notion was further supported by participant J who mentioned the POPIA regulation and the fact that staff had access to customer information, as well as financial information and that "*educating our existing staff*" was essential to ensure that everyone had a collective responsibility to protecting data as well.

5.4.3 Learning from the post incident review process

The post incident review affords an organisation the opportunity to evaluate the entire cyber resilience operationalisation process and discuss any shortcomings or gaps that were identified during an actual adverse cyber event or simulation exercise (Annarelli, Nonino & Palombi, 2020; Sithole, 2019; Linkov & Kott, 2019). According to participant F, it was important to identify these gaps so that the organisation was better positioned to amend or implement new operational tasks that could fill these gaps. Participant F also expressed the need for knowledge sessions, as she had previously gained a lot more exposure and understanding of the technical impacts by participating in such sessions.

Participant G supported that view and stated that as a primary contact point for the cyber resilience process, he would adjust his overall process according to the feedback and knowledge sessions. Due to the fact that "*the world of technology is evolving at such a fast rate, so I think keeping abreast and aware of how the world of resilience is evolving is critical from an external perspective",* he would use the feedback from these sessions to educate himself about the newest technologies and its associated threat vectors, so that he could provide feedback and recommendation to senior leadership within the organisation about possible investments or additional resource requirements.

Many participants felt that these review meetings also allowed both subject matter experts to voice their opinion about any technical or process limitations while also providing the resilience team a platform to objectively provide input about their own experiences during the process (participant A, B, D, and I). According to both participant B and D, traditionally, there would be a split between business and IT and that once voice "*was always louder than the other*", so

certain opinions or recommendations from an IT perspective, were not always considered as part of practice improvement.

Participant E viewed the feedback as critical to improving his role within operationalisation and that it was important to listen to the feedback and continuously improve the current methods being deployed within the operationalisation process:

> "*if you've got the necessary feedback from all the correct stakeholders and you can present it to a governance forum and they can look at it from again, you know an objective view maybe from a different lens and If you've got all that feedback, then I think that's the type of feedback that we rely on"* (Participant E)

Participant K perceived the feedback session to reaffirm that the correct skills were allocated to the resilience team to ensure the structure of the resilience team was practically aligned to deliver the objective of cyber resilience and if that there were knowledge or skills gaps, it be addressed by the resilience team.

Participant L considered the feedback session as an opportunity to look at the legacy technologies in use within the organisation and advocate for the adoption of newer technologies that could assist with legacy issues such as support and availability of skills.

> *"And then obviously the tooling and the that the various services that provide have all of these features of resilience both in you know, so it just makes it a lot easier than having your own handcrafted because you get engineers that come in today, they set up something. But how do you ensure that you have this continuity of the next chain of people that come in over time that can continue to support this."* (Participant L).

5.5 Chapter Summary

This chapter highlights various factors that affect the different phases of the cyber resilience continuum. Risk appetite and business requirements were highlighted by stakeholders as critical aspects that influenced their respective planning processes during the plan phase. These two aspects played a role in assigning priority and resource allocation, to ensure that Company A could meet the objective of cyber resilience, while still meeting business objectives and ensure that the risk was appropriately managed according to the risk profile of Company A.

The importance of data protection and adequacy of testing system resilience were seen as aspects that influenced stakeholders' approach to the absorb phase. The data protection component was highlighted by stakeholders from both a data access and availability perspective. The data access was seen as a risk control to minimise unauthorised access, while the availability of data was crucial to the overall running of business operations during a cyber event. The technical resilience testing requirements of the systems, which support the overall continuity of business operations within Company A, was deemed critical to the success of the absorb phase as it allowed business continuity.

The recovery phase underlined the significance of the impact of recovery time on business operations and the value of data quality as part of recovery phases. The impact of recovery time was deemed important as it directly correlated to the amount of time it would take to recover systems to a workable state. Ensuring the quality of data was not compromised during the recovery process, was also noted as an important facet of the process. The value of the data quality was directly linked to the data recovery part of the process, as the accuracy and completeness of data was important to stakeholders.

The potential impact of artificial intelligence in future, need for more training and awareness, along with the learnings from post incident review process emerged from the adapt phase as aspects that would be top of mind for stakeholders when looking at how to continuously improve and adapt the cyber resilience operationalisation process of Company A. Artificial intelligence was seen as a potential risk in future but also as an enabler for automating certain processes within the cyber resilience process. Training and awareness, as well as post incident review were seen as communication methods which could strengthen the understanding of cyber threats across Company A and contribute towards a better understanding of cyber threats and cyber resilience.

6. Discussion and conclusion

This chapter discusses the findings and how it relates to the research question and objectives. Section 6.1 presents the research objectives. Section 6.2 discusses how the factors influence stakeholder perspectives and practices with regards to cyber resilience, while section 6.3 deals with how the factors and stakeholder perspectives impact organisational cyber resilience operationalisation. Limitation of the study is discussed in section 6.4, while section 6.5 offers possible future research suggestions. The chapter concludes with a final summary in section 6.6.

6.1 Research objectives

The main objective of the research was to identify the factors that influence how cyber resilience is operationalised within organisations. To help answer the main objective, we proposed the following sub objectives:

- To explain which factors influence cyber resilience operationalisation.
- To explain how these factors influence stakeholder perspectives and practices with regards to cyber resilience.
- To explain how these factors and stakeholder perspectives impact cyber resilience operationalisation within an organisation.

To achieve these objectives, an interpretive, qualitative approach was followed in which data was collected through twelve semi-structured interviews with stakeholders from a financial services organisation. The data was analysed using thematic analysis and several themes were uncovered during this process. The codebook and subsequent themes are shown in Annexure E.

The results of this analysis highlighted several factors that influence the operationalisation of cyber resilience from a stakeholder perspective in Company A. These factors and a summary of the factors influencing cyber resilience operationalisation is presented in table 6.1.

Table 6.1: Summary of factors that influence cyber resilience operationalisation

Cyber resilience phase	Factors influencing cyber resilience operationalisation
Plan	Risk appetite
	Business requirements
Absorb	Importance of data protection
	Adequacy of testing system resilience
Recover	Impact of recovery time on business operations
	Value of data quality as part of recovery phase
Adapt	Emerging technology trends
	The need for more training and awareness amongst staff
	Learning from the post incident review process

The following section highlights how these factors influence stakeholder perspectives and practices with regards to cyber resilience within the organisational setting.

6.2 Cyber resilience factors influence stakeholder perspective and practices

Based on the identified factors that influence how cyber resilience is operationalised within Company A, there were two distinct concepts that guided the way these factors influenced stakeholder perspective and its subsequent practice or approach. The two themes were organisational requirements and contextual setting of the organisation.

6.2.1 Organisational requirements

Throughout the four phases of cyber resilience, organisational requirements emerged as a consistent consideration during the decision-making process for stakeholders. These organisational requirements influenced the way in which stakeholder prioritised decisions and resources, to enable the operationalisation of cyber resilience at Company A. These organisational requirements aligned to the cyber resilience matrix framework organisational domains (recall table 3.1), namely, physical, information, cognitive and social domains (Bagheri, Ridley & Williams, 2023).

From a physical, information and cognitive organisational domain, stakeholders emphasised the importance of the risk appetite of the organisation, as well as the business requirements, when making decisions during the plan phase. These decisions would then be operationalised as part of the absorb and recover phases.

These organisational decisions made by stakeholders during the plan phase, laid the basis for the technical and process-based tasks underpinning the absorb and recover operations. These decisions included how to ensure the various departmental functions operated as a unit, to ensure that the organisation balanced both business and cyber resilience requirements during operationalisation.

These operational tasks form part of the planning for cyber resilience, management of security controls and classifying of critical information, which are characteristics of the physical, information and cognitive organisational domains. These factors influenced the way in which stakeholders operationalised their requirements in practice.

To enable these requirements, effective communication amongst stakeholders, staff and external parties was pivotal in enforcing a cyber resilience culture. Stakeholders highlighted these characteristics as part of the focusing on effective training and awareness and communication amongst the diverse organisational disciplines to ensure that Company A met the shared objective of cyber resilience.

6.2.2 Contextual environment of organisation

The contextual environment of an organisation has been considered as a factor that influences cyber resilience, as organisational decisions can be driven by regulatory, risk and industry specific standards and be influenced by leadership, size and digital intensity of the organisation (Tsen, Ko & Slapnicar, 2022).

Company A operates within the financial service industry which have more regulatory requirements and a different risk tolerance level than compared to industries that store no personal or financial information (Dupont, 2019). This contextual factor was highlighted by several stakeholders when discussing the use and processing of customer data within Company A, as data was an important asset due to the sensitive nature of the type of customer information being processed as part of daily operations at Company A. As a result of the type of customer data stored and processed, the data required additional levels of data controls to conform to POPIA.

These factors were stated as points that were considered for decisions in both the absorb and recover phases and influenced the way in which stakeholders approach any data protection and other operational regulatory requirements. The digital, customer facing nature of the business and the fact that Company A formed part of a larger banking group, were also considered by several stakeholders as important contextual environmental considerations in ensuring compliance to industry regulations to minimise both reputational damage and regulatory fines.

6.3 Impact of factors on resilience operationalisation within the organisation

The analysis of the data presented in Chapter 5 also identified the impact these cyber resilience factors have on the organisation. A summary of the factors and the associated impact these factors have on the operationalisation of cyber resilience within the organisation is presented in table 6.2.

Table 6.2: Summary of factors that influence cyber resilience operationalisation and its impact on the organisation.

Cyber resilience phase	Factors influencing cyber resilience	Impact of factors on resilience operationalisation within the organisation
Plan	Risk appetite	Prioritisation is key in cyber resilience operationalisation Resource availability determines priorities and organisational focus Internal and external factors impact organisational considerations Continuous improvement of cyber resilience as a practice is critical to ensure its ongoing effectiveness
	Business requirements	
Absorb	Importance of data protection	
	Adequacy of testing system resilience	
Recover	Impact of recovery time on business operations	
	Value of data quality as part of recovery phase	
Adapt	Emerging technology trends – Impact of AI	
	The need for more training and awareness amongst staff	
	Learning from the post incident review process	

The impact of these factors on the operationalisation of cyber resilience within the organisation became evident with the emergence of four key themes, namely, organisational prioritisation, resource allocation, customer trust and continuous improvement of cyber resilience as a practice. The following sections provide insight into each one of these themes.

6.3.1 Prioritisation is key in cyber resilience operationalisation

Prioritisation emerged as a theme that was necessitated by the impact of several cyber resilience factors such as business requirements, risk appetite and the technical testing process. Each of these factors had an impact on the organisational prioritisation for cyber resilience within the organisation.

Business requirements emerged as a factor that was key to the way stakeholders prioritised their planning requirements. These business requirements were informed by both internal and external factors. Several participants mentioned how internal factors such as a change in business direction or a change in requirements from a Group level, would then necessitate a change in prioritisation at Company A. When such changes in prioritisation are brought on by internal factors such as shifts in the direction of the business or Group level mandated changes, there is often an impact in implementation decisions within organisations (Tsen, Ko & Slapnicar, 2022).

From an external factor perspective, an example of a shift in business requirements highlighted by participant E, involved a scenario where a cyber threat could evolve from a simple to more sophisticated attack and would therefore require either more computing resources being directed to different levels of a system or needing more diverse technical resources to assist in preparing for such an attack. This would result in the prioritisation changing as a result of the emergence of a more advanced attack. Another participant also mentioned how changes could be trigged by macroeconomic elements, which also forms part of external factors that impact business requirements or changes in technology risk, which can result in risk to an organisation (Assibi, 2023).

These internal and external factors contribute towards changes in prioritisation within Company A and should therefore be considered when preparing the initial phases of cyber resilience, as the impact on operationalisation can be showed in both technical and operational processes.

Any material change in risk appetite would impact the way stakeholders would prioritise planning for the various cyber threat scenarios based on the risk categories within Company A. These changes in the risk appetite would impact the structuring of operational processes which support the objective of cyber resilience or shifting the technical prioritisation between the different teams within the organisation. This alignment of organisational resources to support a change in priority, also assists in ensuring the organisation can adjust their resilience to counter evolving threats (Jeimy & Cano, 2023).

6.3.2 Resource availability determines priorities and organisational focus

The availability of resources to implement and manage the operationalisation process within Company A, was highlighted by several stakeholders as an important consideration during the plan phase and also emerged as a consideration in the absorb phase, when allocating resources to perform tailored technical testing on the selected systems. Due to the integrated nature of cyber resilience, a diverse set of stakeholders from various departmental disciplines are required to work together, to ensure that the operationalisation of cyber resilience is achieved. Due to the different interests of stakeholders (Recall chapter 2.1), there are several challenges associated with this form of collaboration including the availability of resourcing (Munusamy & Khodadi, 2023; Sithole, 2019).

Several stakeholders emphasized the importance of risk appetite as a fundamental factor which provided them with a reference point for their approach to implementing operational and technical processes that support the objective of cyber resilience. These include having the required resources available to implement and support the process during the plan phase and ensuring that the correct resources and focus was allocated to the various interdependent tasks. The importance of having resources available has also been highlighted in literature as paramount to the entire cyber resilience process (Tarhini, 2015; Scolobig & Lilliestam, 2016) and has also been highlighted in the ISO 22316 security and resilience standard, which provides principles and guidelines to establish organisational resilience, as a key attribute (Munusamy & Khodadi, 2023).

Participants from the risk department emphasized that it was crucial for adequate testing to be performed as the objective of cyber resilience was to ensure systems were able to absorb the impact of the cyber threats produced by the risk assessments. Failure of systems to recover to an active state would negatively impact Company A's ability to operate and render the cyber resilience process mute.

From a technical perspective, several participants in the IT department highlighted the risk of a change or deviation in system design and there would be a direct impact on the technical requirements for each test. This was important as technical requirements were tailored to ensure resilience and changes would impact whether a system could withstand a cyber event. If a test failed due to the testing methods not being fit for purposes, there would be no form of assurance that the organisation systems met the threshold to be considered resilient (Bagheri, 2020).

The overall success of the operationalisation process would be hindered by the unavailability of resources, possibly resulting in improper allocation of other resources to complete operational tasks.

The absence of sufficient resources would place constraints on the organisation and negatively impact the effectiveness of the entire cyber resilience process.

6.3.3 Internal and external factors impact organisational considerations

From a data protection perspective, stakeholders referred to data access and data availability as important to ensure that the risk to customer information at Company A was minimised. Data protection plays a crucial role in organisations based in the financial sector where personal information is processed and stored as part of its operational processes (Dupont, 2019). These requirements of availability and access control form part of overall information security and data protection principles (Stamp, 2011). From a South African context, the POPIA regulation governs the protection of personal information and this regulation was mentioned by a few participants as part of the reason why data protection was important to Company A. The researcher also noted references to POPIA and other financial regulations in some of the documentation that was perused as part of the secondary data that was analysed.

These industry regulations formed the basis of the data protection process at Company A. Participant J provided an example and noted that changes to data classification would impact the type of access assigned to staff processing data on a system and it was essential to ensure that limited access was provided at a user level. Another participant highlighted the importance of data being available for both operational requirements and customer services, to ensure some form of assurance, or trust, in the data, especially when dealing with both personal and transactional information.

In both instances, the impact of not having adequate data protection principles in place, would lead to unauthorised access to data and reputational damage due a lack of trust from customers about whether their personal information was adequately secured. The importance of data protection can therefore not be neglected as data breaches have often proven to be damaging both financially and reputational (Dupont, 2019; Carayannis et al., 2019).

Another factor that impacted customer trust, was the impact of recovery time on the operational impact of business processes. The downtime on business operations can be translated into downtime and the more downtime there is, the higher the loss of revenue, reputational damage and erosion of customer trust in the brand of the organisation (Estay et al., 2020; Dupont, 2019).

Linked to the impact of recovery time on business processes, participants involved with the daily operations of the company highlighted the need for assurances of the accuracy of the data to ensure that Company A could trust the accuracy of the data to perform daily analytical routines.

The growth in the use of data for business purposes over the past decade, has also put a spotlight on the processing and protection of data globally and necessitated the need for data to be a vocal point of many security strategies (Fischer-Hübner et al., 2021).

This type of impact to the business operations, was noted as a major risk amongst several participants who expressed concern about any failure during the recovery process of business-critical systems. If customer data was not available or if the system was not recovered to a certain extent where it could service customers, then no business activities could commence and that would impact customer trust levels (Sithole, 2019).

Since Company A operated in a customer services space within the financial sector, there were regulatory requirements that could also potentially impact the company in terms of fines and therefore recovery time and its direct impact on business processes from a cyber threat, was deemed critical to participants.

6.3.4 Continuous improvement of cyber resilience as a practice is critical to ensure its ongoing effectiveness

There were several factors that were identified as contributing to the continuous improvement and enhancement of the cyber resilience practice. The flexibility and adaptability for an organisation to pivot during unforeseen events, provide an opportunity to identify opportunities for enhancements in processes to cater for future scenarios (Dupont, 2019; Annarelli, Nonino & Palombi, 2021).

The growth of AI and its practical application in the form of prompt applications like ChatGPT, sparked debate from participants to whether this would have a positive or negative impact on Company A. The discourse about the practical implications of AI within organisations from a cyber resilience perspective, have been highlighted in several cyber resilience publications over the past few years (Annarelli, Nonino & Palombi, 2021; Carayannis et al., 2019; Hausken, 2020).

From a threat perspective, several participants expressed concern about how prompt applications like ChatGPT could provide threat actors information on how to develop or look for exploits that can be used in a cyber-attack. In essence, these AI applications could provide information about how to circumvent security controls and place organisations in a vulnerable position, having to mitigate additional risks that may not have been previously applicable. This would have an impact on the way Company A would plan its cyber resilience processes, as it had to look at the additional threats suggested by AI.

From an enabling perspective, some participants saw AI as a useful tool that could automate and speed up some of the more cumbersome processes that needed manual intervention as part of operational process checks. As stated by one participant, AI could help speed up

certain tests to check the accuracy of data and do a comparative check that the data or processes were running appropriately as before an attack occurred. Automation could therefore also positively contribute to the overall cyber resilience process.

To ensure that an organisation continuously adapts to the continuous shift in cyber threats, the adapt phase provides the organisation with an opportunity to review test plans and actual incidents and identify areas requiring improvement or reconfiguration (Annarelli & Palombi, 2021). The post incident review is a process that Company A uses to address any shortcomings during their testing phase. This form of review was perceived by stakeholders as the process from which they derived the most value, since all participants who formed part of cyber resilience process, was given an opportunity to address issues from their vantage points. The input from various stakeholders provided a holistic end to end view of the cyber resilience process to identify any risks or potential gaps, which can augment and strengthen the operationalisation process.

As part of the post incident review process, training and awareness were perceived by participants as important to the overall improvement of the cyber security posture of Company A. Training and awareness provided staff information regarding the importance of cyber security and strengthening the collective responsibility of ensuring security culture across Company A. This in turn would have a positive impact on the levels of understanding regarding cyber threats amongst staff and therefore increase the awareness levels, especially for staff that play a role in operationalisation aspect of cyber resilience.

6.4 Limitations of study

The study was limited to one organisation within the financial services sector in Cape Town and therefore the results of this research was based on one, singular case study. Due to the time restriction imposed by the requirement for the master's degree, there was not enough time to collect data from another organisation within a different sector for a comparative view of factors which could expand on the generalisability of the research.

The results are qualitative in nature and therefore do not claim any statistical significance as part of this study. This study also focused on one set of stakeholders, which were the employees of the organisation and did not include other stakeholders which could have generated other insights as part of the research.

6.5 Future research

Due to the limitations of only being able to utilise one organisation within one industry, future studies could use the findings of this research to compare factors that that influence cyber resilience operationalisation in organisations from different sectors within South Africa. Such studies can help expand the amount of available empirical data and provide greater insight into the various factors that influence cyber resilience operationalisation across different sectors and geographical locations across South Africa.

Another area of future research, given the expansive and rapid adoption of AI, is the impact of AI on cyber resilience operationalisation. Considering the speed at which AI can consume data and produce statistical and contextual information, further studies can look at how AI can be used to complement, automate or predict events which could positively or negatively impact the way cyber resilience is currently structured and operationalised within organisations.

6.6 Final summary

This research set out to identify which factors influence how cyber resilience is operationalised from a stakeholder perspective within organisations. Literature highlights the importance of stakeholder involvement in achieving the objective of cyber resilience through enabling a collaborative, uniformed approach to operationalisation. The researcher used the cyber resilience matrix framework as a lens to identify the factors that influence cyber resilience operationalisation within organisation, as well as the impact these factors have on the operationalisation of cyber resilience within the organisation. Through a semi-structured interview process, several stakeholders provided their perspectives on cyber resilience operationalisation and thematic analysis was used to analyse the collected data.

Risk appetite and business requirements were identified as factors that influenced the operationalisation of cyber resilience during the plan phase. These factors were found to have an impact on the resource availability for operationalisation, as well as organisational prioritisation.

The importance of data protection and having a tailored, fit for purpose resilience testing were identified as factors that shaped stakeholder perspectives during the absorb phase. The impact of industry regulation data protection principles on the use of data within Company A, was deemed critical for managing reputational damage and loss of customer trust. In terms of technical resilience testing, it was key to ensure that the testing methods were suitable and customized to the organisation's requirements, to ensure correct prioritisation and allocation of suitable resources. This ensured that business-critical systems could continue functioning after the impact of a cyber threat and meet the objective of cyber resilience.

During the recovery phase, stakeholders' perspectives were influenced by two factors: the impact of recovery time and the value of data quality as part of the recovery process. The impact of recovery time was measured in terms of overall impact on business processes that support the operations of Company A. This impact was measured in respect of the time it took for a company to resume their business operations and linked to that, the assurance that the quality and integrity of the data was intact, which provided a level of reassurance and trust to external stakeholders such as customers and the wider Group, that the company was in a functional state.

Emerging technology trends, especially AI, training and awareness of cyber resilience amongst staff and post incident review process were highlighted by stakeholders as important factors that influenced the adapt phase. These factors were considered central in the drive to continuously improve the cyber operationalisation process within Company A and pivotal in ensuring continual adaptability against the future of cyber based threats.

References

Adams, R., Adeleke, F., Anderson, D., Bawa, A., Branson, N., Christoffels, A., ... & Ramsay, M. (2021). POPIA code of conduct for research. South African Journal of Science, 117(5-6), 1-12.

Annarelli, A., & Palombi, G. (2021). Digitalization Capabilities for Sustainable Cyber Resilience: A Conceptual Framework. *Sustainability*, *13*(23), 13065.

Annarelli, A., Nonino, F., & Palombi, G. (2020). Understanding the management of cyber resilient systems. *Computers & industrial engineering*, *149*, 106829.

Assibi, A. T. (2023). Literature Review on Building Cyber Resilience Capabilities to Counter Future Cyber Threats: The Role of Enterprise Risk Management (ERM) and Business Continuity (BC). *Open Access Library Journal*, *10*(4), 1-15.

Bagheri, S. (2020). *Investigating organisational aspects of cyber resilience in large organisations* (Doctoral dissertation, University Of Tasmania).

Bagheri, S., Ridley, G., & Williams, B. (2023). Organisational Cyber Resilience: Management Perspectives. *Australasian Journal of Information Systems*, *27*.

Beaver, W. (1999). Is the stakeholder model dead? *Business Horizons*, *42*(2), 8-13.

Bhattacherjee. (2012). *Social science research: principles, methods, and practices*. Global Text Project.

Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber resilience–fundamentals for a definition. *In New contributions in information systems and technologies* (pp. 311-316). Springer, Cham.

Board, F. S. (2013). Principles for an effective risk appetite framework. Consultative Document, July.

Bodeau, D. J., Graubart, R., Picciotto, J., & McQuaid, R. (2011). *Cyber resiliency engineering framework*. MITRE CORP BEDFORD MA.

Bodeau, D. J., Graubart, R. D., McQuaid, R. M., & Woodill, J. (2018). *Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring: Enabling Systems Engineers and Program Managers to Select the Most Useful Assessment Methods*. Mitre Corp Bedford Ma Bedford United States.

Boonstra, A. (2006). Interpreting an ERP-implementation project from a stakeholder perspective. *International journal of project management*, *24*(1), 38-52.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, *3*(2), 77-101.

Brunetti, F., Matt, D. T., Bonfanti, A., De Longhi, A., Pedrini, G., & Orzes, G. (2020). Digital transformation challenges: strategies emerging from a multi-stakeholder approach. *The TQM Journal*, *32*(4), 697-724.

Bryson, M. (1995). John, Strategic Planning for Public and Nonprofit Organizations. A Guide to Strengthening and Sustaining Organizational Achievement.

Buchmann, R. A., Polini, A., Johansson, B., & Karagiannis, D. (Eds.). (2020). Perspectives in Business Informatics Research: 19th International Conference on Business Informatics Research, BIR 2020, Vienna, Austria, September 21–23, 2020, Proceedings (Vol. 398). Springer Nature.

Burstein, M., Goldman, R., Robertson, P., Laddaga, R., Balzer, R., Goldman, N., ... & Wile, D. (2012, September). Stratus: Strategic and tactical resiliency against threats to ubiquitous systems. In *2012 IEEE Sixth International Conference on Self-Adaptive and Self-Organizing Systems Workshops* (pp. 47-54). IEEE.

Bunn, M. D., Azmi, F., & Puentes, M. (2009). Stakeholder perspectives and implications for technology marketing in multi-sector innovations: the case of intelligent transport systems. *International Journal of Technology Marketing*, *4*(2-3), 129-148.

Carayannis, E. G., Grigoroudis, E., Rehman, S. S., & Samarakoon, N. (2019). Ambidextrous cybersecurity: The seven pillars (7Ps) of cyber resilience. *IEEE transactions on engineering management*, *68*(1), 223-234.

Carías Alvarez, J. F. (2021). Cyber Resilience Operationalization Framework *(CR-OF)* for SMEs.

Carías, J. F., Arrizabalaga, S., Labaka, L., & Hernantes, J. (2020). Cyber resilience progression model. *Applied Sciences*, *10*(21), 7393.

Carías, J. F., Borges, M. R., Labaka, L., Arrizabalaga, S., & Hernantes, J. (2020). Systematic approach to cyber resilience operationalization in SMEs. *IEEE Access*, 8, 174200-174221.

Carter, W. (2017). Forces shaping the cyber threat landscape for financial institutions.

Castillo-Montoya, M. (2016). Preparing for interview research: The interview protocol refinement framework. *Qualitative report*, *21*(5).

Chatterjee, D. (2021). *Cybersecurity readiness: A holistic and high-performance approach*. SAGE Publications.

CISCO. 2023. *CISCO Cybersecurity Readiness Index.* Retrieved September 23, 2023, from CISCO: https://www.cisco.com/c/dam/m/en_us/products/security/cybersecurity-reports/cybersecurity-readiness-index/2023/cybersecurity-readiness-index-report.pdf

Clausmeier, D. (2023). Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA). International Cybersecurity Law Review, 4(1), 79-90.

Colabianchi, S., Costantino, F., Di Gravio, G., Nonino, F., & Patriarca, R. (2021). Discussing resilience in the context of cyber physical systems. *Computers & Industrial Engineering*, 160, 107534.

Colicchia, C., Creazza, A., & Menachof, D. A. (2019). Managing cyber and information risks in supply chains: insights from an exploratory analysis. *Supply Chain Management: An International Journal*, *24*(2), 215-240.

Collier, Z. A., DiMase, D., Walters, S., Tehranipoor, M. M., Lambert, J. H., & Linkov, I. (2014). Cybersecurity standards: Managing risk and creating resilience. *Computer*, *47*(9), 70-76.

Connelly, E. B., Allen, C. R., Hatfield, K., Palma-Oliveira, J. M., Woods, D. D., & Linkov, I. (2017). Features of resilience. Environment Systems and Decisions, 37(1), 46–50.

Crane, B. (2020). Revisiting who, when, and why stakeholders matter: Trust and stakeholder connectedness. Business & Society, 59(2), 263-286.

Dalton, W., van Vuuren, J. J., & Westcott, J. (2017). Building cybersecurity resilience in Africa. In *12th International Conference on Cyber Warfare and Security* (pp. 112-120).

Dickson, F., & Goodwin, P. (2020). Five key technologies for enabling a Cyber-resilience framework. *US45455119, IBM, White Paper*.

Donaldson, T., & Preston, L. E. (1995). The stakeholder theory of the corporation: Concepts, evidence, and implications. *Academy of management Review*, *20*(1), 65-91.

Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. *Journal of cybersecurity*, *5*(1), tyz013.

Dupont, B., Shearing, C., Bernier, M., & Leukfeldt, R. (2023). The tensions of cyber-resilience: From sensemaking to practice. Computers & Security, 132, 103372.

Elo, S., Kääriäinen, M., Kanste, O., Pölkki, T., Utriainen, K., & Kyngäs, H. (2014). Qualitative Content Analysis: A Focus on Trustworthiness. *SAGE Open*.

Estay, D. A. S., Sahay, R., Barfod, M. B., & Jensen, C. D. (2020). A systematic review of cyber-resilience assessment frameworks*. Computers & security*, 97, 101996.

Fischer-Hübner, S., Alcaraz, C., Ferreira, A., Fernandez-Gago, C., Lopez, J., Markatos, E., ... & Akil, M. (2021). Stakeholder perspectives and requirements on cybersecurity in Europe. *Journal of information security and applications*, *61*, 102916.

Florea, R., & Florea, R. (2013). Stakeholders interests analyse and harmonization-starting point of strategic approach. *Economy Transdisciplinarity Cognition*, *16*(1), 130.

Freeman, R. E., & McVea, J. (2001). A stakeholder approach to strategic management. M. Hitt, E.

Forero, R., Nahidi, S., De Costa, J., Mohsin, M., Fitzgerald, G., Gibson, N., McCarthy, S., & Aboagye-Sarfo, P. (2018). Application of four-dimension criteria to assess rigour of qualitative research in emergency medicine. BMC health services research, 18(1), 120. https://doi.org/10.1186/s12913-018-2915-2

Frooman, J. (1999). Stakeholder influence strategies. *Academy of management review*, *24*(2), 191-205.

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The qualitative report*, *8*(4), 597-607.

Graubart, R., & Bodeau, D. (2016). *Cyber resilience metrics: Key observations*. MITRE corp Mclean VA Mclean.

Greiman, V. A. and Bernardin, E. (2021) Cyber Resilience: A Global Challenge. Academic Conferences and Publishing Ltd. (ACPIL), Reading, UK.

Haimes, Y. Y. (2009). On the definition of resilience in systems. *Risk Analysis: An International Journal*, *29*(4).

Haki, K., Aier, S., & Winter, R. (2016). A stakeholder perspective to study enterprisewide IS initiatives.

Harrison, J. S., & van der Laan Smith, J. (2015). Responsible accounting for stakeholders. *Journal of Management Studies*, *52*(7), 935-960.

Harper, G. R., & Utley, D. R. (2001). Organisational culture and successful information technology implementation. *Engineering Management Journal*, *13*(2), 11-15.

Hausken, K. (2020). Cyber resilience in firms, organisations and societies. *Internet of Things*, 11, 100204.

IBM. 2023. *Cost of a data breach report*. Retrieved October 11, 2023, from IBM: https://www.ibm.com/reports/databreach#:~:text=The%20global%20average%20cost%20of,15%25%20increase%20over%203%20years.&text=51%25%20of%20organisations%20are%20planning,threat%20detection%20and%20response%20tools.

Iyamu, T., & Batyashe, N. R. (2020). Operationalisation of the Information Technology strategy in an organisation. *Journal of Contemporary Management*, *17*(2), 198-224.

Jeimy, J., & Cano, M. (2023). FLEXI-A Conceptual Model for Enterprise Cyber Resilience. Procedia Computer Science, 219, 11-19.

Kim, Y., & Crowston, K. (2011). Technology adoption and use theory review for studying scientists' continued use of cyber-infrastructure. *Proceedings of the American Society for Information Science and Technology*, *48*(1), 1-10.

Ligo, A. K., Kott, A., & Linkov, I. (2021). How to measure cyber-resilience of a system with autonomous agents: Approaches and challenges. *IEEE Engineering Management Review*, *49*(2), 89-97.

Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions*, *33*(4), 471-476.

Linkov, I., & Kott, A. (2019). Fundamental concepts of cyber resilience: Introduction and overview. *In Cyber resilience of systems and networks* (pp. 1-25). Springer, Cham.

Liquid Technologies. 2022. *The evolving cybersecurity landscape in Africa.* Retrieved September 7, 2023, from Liquid Technologies: https://liquid.tech/wp-content/uploads/2023/06/LIQUID-C2-Report.pdf

Loonam, J., Zwiegelaar, J., Kumar, V., & Booth, C. (2020). Cyber-Resiliency for Digital Enterprises: A Strategic Leadership Perspective. *IEEE Transactions on Engineering Management*.

Ma, Z., Xiao, L., & Yin, J. (2018). Toward a dynamic model of organisational resilience. *Nankai Business Review International*, *9*(3), 246-263.

Machan, T. R. (2017). Stakeholder vs. shareholder debate: Some skeptical reflections. Contemporary Readings in Law and Social Justice, 9(1), 7-13.

Marchese, D., Jin, A., Fox-Lent, C., & Linkov, I. (2020). Resilience for smart water systems. Journal of Water Resources Planning and Management, 146(1), 02519002.

Maurer, T., & Nelson, A. (2020). International strategy to better protect the financial system against cyber threats. Washington DC: Carnegie Endowment for International Peace.

Mishra, A., & Mishra, D. (2013). Applications of stakeholder theory in information systems and technology. *Engineering Economics*, *24*(3), 254-266.

Microsoft. 2023. *Microsoft Digital Defense report*. Retrieved October 19, 2023, from Microsoft: https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

Munusamy, T., & Khodadi, T. (2023). Building Cyber Resilience: Key Factors for Enhancing Organisational Cyber Security. *Journal of Informatics and Web Engineering*, *2*(2), 59-71.

Neeme, S. (2022). Cyber resilience: A global challenge.

Onwubiko, C. (2020, June). Focusing on the recovery aspects of cyber resilience. In *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)* (pp. 1-13). IEEE.

Pavão, J., Bastardo, R., Carreira, D., & Rocha, N. P. (2023). Cyber Resilience, a Survey of Case Studies. *Procedia Computer Science*, *219*, 312-318.

Patton, M. Q. (2014). *Qualitative research & evaluation methods: Integrating theory and practice*. Sage publications.

Petrenko, S. (2022). *Cyber resilience*. CRC Press.

Peter, Ada S. "Cyber resilience preparedness of Africa's top-12 emerging economies." *International Journal of Critical Infrastructure Protection* 17 (2017): 49-59.

Pieterse, H. (2021). The cyber threat landscape in South Africa: A 10-year review. *The African Journal of Information and Communication*, *28*, 1-21.

Pomerleau, P. L., & Lowery, D. L. (2020). Countering Cyber Threats to Financial Institutions. In A Private and Public Partnership Approach to Critical Infrastructure Protection. Springer.

Rand, K., Kurth, M., Fleming, C. H., & Linkov, I. (2020). A resilience matrix approach for measuring and mitigating disaster-induced population displacement. *International journal of disaster risk reduction*, *42*, 101310.

Reed, M. S. (2008). Stakeholder participation for environmental management: a literature review. *Biological conservation*, *141*(10), 2417-2431.

Refsdal, A., Solhaug, B., Stølen, K. (2015). *Cyber-risk management* (pp. 33-47). Springer International Publishing.

Sabev, S. I. (2020). Integrated Approach to Cyber Defence: Human in the Loop. Technical Evaluation Report. Information & Security: An International Journal, 44, 76-92.

Saunders, Lewis, P., & Thornhill, A. (2019). *Research methods for business students* (Eighth edition.). Pearson.

Scholes, K., Johnson, G., & Whittington, R. (2002). *Exploring corporate strategy*. Hoboken, NJ, USA: Financial Times Prentice Hall.

Scolobig, A., & Lilliestam, J. (2016). Comparing approaches for the integration of stakeholder perspectives in environmental decision making. Resources, 5(4), 37.

Sentinel One.2023. *Cyber Attacks on Financial Institutions | Why Banks Are Caught in the Crosshairs*. Retrieved September 7, 2023, from Sentinel One: https://www.sentinelone.com/blog/a-cyberwar-on-financial-institutions-why-banks-are-caught-in-the-crosshairs/

Sithole, T. G. (2019). *Assessing resilience of public sector Information Systems against cyber threats and attacks. A South African perspective* (Doctoral dissertation, University of Pretoria).

Smith, S. (2023, February). Towards a scientific definition of cyber resilience. In *International Conference on Cyber Warfare and Security* (Vol. 18, No. 1, pp. 379-386).

Stamp, M. (2011). *Information security: principles and practice*. John Wiley & Sons.

Stine, K., Quinn, S., Witte, G., & Gardner, R. K. (2020). Integrating cybersecurity and enterprise risk management (ERM). *National Institute of Standards and Technology*, *10*.

Tarhini, A., Ammar, H., Tarhini, T., & Masa'deh, R. E. (2015). Analysis of the critical success factors for enterprise resource planning implementation from stakeholders' perspective: A systematic review. *International Business Research*, *8*(4), 25-40.

Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. Computers & Security, 109, 102387.

Wahyuni, D. (2012). The research design maze: Understanding paradigms, cases, methods and methodologies. *Journal of applied management accounting research*, *10*(1), 69-80.

Wells, E. M., Boden, M., Tseytlin, I., & Linkov, I. (2022). Modeling critical infrastructure resilience under compounding threats: A systematic literature review. Progress in Disaster Science, 100244.

Werth, H. (2019). *Stakeholder perspectives of organisational response to crisis: a case study* (Doctoral dissertation, Stellenbosch: Stellenbosch University).

Zemba, V., Wells, E. M., Wood, M. D., Trump, B. D., Boyle, B., Blue, S., ... & Linkov, I. (2019). Defining, measuring, and enhancing resilience for small groups. *Safety Science*, 120, 603-616.

Annexure A – Ethics approval

Faculty of Commerce
Private Bag X3, Rondebosch, 7701
2.26 Leslie Commerce Building, Upper Campus
Tel: +27 (0) 21 650 4375/ 5748 Fax: +27 (0) 21 650 4369
E-mail: jacques.rousseau@uct.ac.za
Internet: www.uct.ac.za
@Commerce UCT UCT Commerce Faculty Office

15 01 2023

Asterico Adams

Department of Information Systems

University of Cape Town

REF: REC 2023/01/006

Investigating the effect of stakeholder perception on organisational cyber resilience operationalisation – A financial organisational case study

We are pleased to inform you that your ethics application has been approved. Unless otherwise specified this ethical clearance is valid until 31-Jan-2024 .

Your clearance may be renewed upon application.

Please be aware that you need to notify the Ethics Committee immediately should any aspect of your study regarding the engagement with participants as approved in this application, change. This may include aspects such as changes to the research design, questionnaires, or choice of participants.

The ongoing ethical conduct throughout the duration of the study remains the responsibility of the principal investigator.

We wish you well for your research.

Signed by candidate 2023.01.15 19:49:23 +02'00'

Jacques Rousseau
Commerce Research Ethics Chair
University of Cape Town
Commerce Faculty Office
Room 2.26 | Leslie Commerce Building

Office Telephone: +27 (0)21 650 2695 / 4375
Office Fax: +27 (0)21 650 4369
E-mail: jacques.rousseau@uct.ac.za
Website: http://www.commerce.uct.ac.za/com/Ethics-in-Research

"Our Mission is to be an outstanding teaching and research university, educating for life and addressing the challenges facing our society."

Annexure B – Research letter

Department of Information Systems
Leslie Commerce Building
Engineering Mall, Upper Campus
OR
Private Bag X3 - Rondebosch - 7701
Tel: +27 (0) 21 650 2261 Fax: +27 (0) 21650 2280
Internet: http://www.commerce.uct.ac.za/informationsystems/

16 November 2022

Request to conduct research and interview participation consent form

Dear Sir/Madam,

In terms of the requirements for completing a Masters Degree in Information Systems at the University of Cape Town a research study is required.

The researcher, in this case Asterico Adams, has chosen to conduct a case study entitled *Investigating the effect of stakeholder perception on cyber resilience operationalisation – A financial organisational case study*. The objective of the research is to understand how stakeholder perception affect the objective of cyber resilience operationalisation.

Your participation in this research is voluntary. All information will be treated in a confidential manner and used exclusively for the purpose of this study. No individual names will be recorded or published. You will not be requested to supply any identifiable information, ensuring anonymity of your responses. You can choose to withdraw from the research at any time for whatever reason, in accordance with ethical research requirements.

The data collection method will be one-on-one interviews with a small group of stakeholders responsible for cyber resilience operationalisation. The interviews will be conducted at the premises of the company and will last approximately one hour. If you are willing to participate in this study, kindly sign the attached form and return to me at your earliest convenience.

Should you have any questions regarding this research, please feel free to contact me on 082 727 5224 or email: admast001@uct.ac.za

Your participation in this study would be greatly appreciated, but is entirely voluntary.

Sincerely,

Signed by candidate

Signed by candidate

Asterico Adams
Researcher \ M.Com Student, (UCT)
Department of Information Systems
University of Cape Town
Email: admast001@uct.ac.za

Professor Wallace Chigona
Research Supervisor
Department of Information Systems
University of Cape Town
Email:

Annexure C – Consent Form

Department of Information Systems
Leslie Commerce Building
Engineering Mall, Upper Campus
OR
Private Bag X3 - Rondebosch - 7701
Tel: +27 (0) 21 650 2261 Fax: +27 (0) 21650 2280
Internet: http://www.commerce.uct.ac.za/informationsystems/

Research Participant Consent Form

I, _____, consent to participate in the research on Investigating the effect of stakeholder perception on cyber resilience operationalisation – A financial organisational case study.

I am aware that participation is voluntary and that I may choose to withdraw from this study at any time, should I choose to do so.

_____ _____

Signature Date

Annexure D – Semi-Structured Interview Protocol

Opening questions

1. What is your current role and main area of responsibility within the organisation?
2. How long have you been in your current role at the organisation and how many years of experience do you have within this type of role/domain overall?
3. What do you know about the concept of cyber resilience?
4. What are your thoughts on the need for cyber resilience?
5. How does cyber resilience add value to the organisation?

Plan/Prepare Phase

6. How do you plan or map out your responsibilities from a policy, standard or process perspective, when it comes to cyber resilience implementation?
7. How do you determine the order of priorities as part of your planning?
8. What would influence a change in your priorities?
9. Are there any specific frameworks, models or industry standards you reference when it comes to planning for cyber resilience operationalisation? If you do, why that specific one? If not, why not?

Absorb/Withstand Phase

10. What informs your decision when it comes to selecting the systems or business processes which need to be risk mitigated as part of cyber resilience operationalisation?
11. What advantages do you believe comes from being able to keep the systems up and running during a cyber event?
12. What concerns you the most when it comes to the process of ensuring systems are adequately tested for resilience? What are those concerns based on?
13. What type of impact do you believe a failed system test would have on the organisation?

Recovery Phase

14. How do you measure the recovery of a system?
15. How do you determine who or what gets involved as part of the recovery process?
16. What type of success factors do you look for when deciding whether a system has recovered to a working state during a cyber event?
17. Why are those factors important to you?

Adapt Phase

18. What type of post incident feedback provides you the most value and why?
19. Which elements (internal or external factors) do you believe needs to be taken into account to ensure the continuous evolving of cyber resilience operationalisation within the organisation?
20. Which areas or aspects of the current organisation cyber resilience operationalisation plan do you believe require more effort or better clarification? Why do you say that?
21. If you had the opportunity to change the current operational model, how differently would you structure cyber resilience operationalisation and why?

Annexure E – Coding Manual

Theme	Codes
Risk appetite	Risk alignment Risk policies Management of risk
Business requirements	Business direction Business objectives Alignment to business
Importance of data protection	Data exposure Customer data Privacy risk Focus on data transfer mechanisms
Adequacy of testing system resilience	Scenario based testing Testing correct systems Regular testing Standard of testing
Impact of recovery time on business operations	Uptime of systems Business up and running Speed of recovery Time taken to recover
Value of data quality as part of recovery phase	Minimal data loss Testing of data quality Data accuracy
The potential impact of artificial intelligence in future	Threat of artificial intelligence Artificial intelligence as an enabler
The need for more training and awareness amongst staff	Staff training Cyber resilience awareness Improving skills levels of staff
Learning from the post incident review process	Knowledge sessions Technical feedback Improvement of entire process