CYBER GOVERNANCE IN THE WATER SECTOR

Volume 3 – Water sector cybersecurity resilience strategy and assessment findings

Report to the
WATER RESEARCH COMMISSION

by

Masike Malatji, Annlizé L. Marnewick, Suné von Solms & Wikus Erasmus
University of Johannesburg

WRC Report No. 3060/3/22
ISBN 978-0-6392-0365-2

March 2023

Obtainable from
Water research Commission
Bloukrans Building
Lynnwood Bridge Office Park
4 Daventry Road
Lynnwood Manor
PRETORIA

orders@wrc.org.za or download from www.wrc.org.za

This report forms part of a set of four reports as part of WRC project no. C2021/23-00354.

The other reports are:

Cyber Governance in the Water Sector. Volume 1: Water and sanitation cybersecurity legislative and policy environment (WRC Report No. 3060/1/22).
Cyber Governance in the Water Sector. Volume 2: Cybersecurity governance framework for the water sector of South Africa (WRC Report No. 3060/2/22)
Cyber Governance in the Water Sector. Volume 4: Education and awareness guidelines (WRC Report No. 3060/4/22)

EXECUTIVE SUMMARY

BACKGROUND

A wide range of corporate information technology (IT) and operational technology (OT) cybersecurity threats and vulnerabilities in the water sector have been identified by both industry and academia. Some are associated with municipal water distribution systems that can easily be sabotaged or even damaged by means of contamination injection, cyberattack or physical destruction (Janke, Tryby & Clark, 2014). In many countries, as in South Africa, critical infrastructure (CI) owners have focused largely on physical security. However, with the increased connectivity through digital technologies and communication networks, cybersecurity has become an area of increasing concern. This is also true of the water and sanitation sector as utilities are increasingly using smart or connected industrial control systems (ICS) for their operational technologies. These are essential for the monitoring and control of physical processes essential to water treatment plants and distribution systems.

Although no credible register of cyber incidents or successful cyberattacks exists in South Africa, it is known that key installations of the country, including the water and sanitation CI, are being targeted. It is therefore prudent for the sector to holistically examine its cybersecurity resilience level, from legislation and policies to governance and capability, and from everyday practices to awareness.

In addition to the water and sanitation sector cybersecurity resilience assessments, a record of the typical cybersecurity incidents (unsuccessful threats) and events (successful attacks) experienced by the sector has been compiled in this report.

RATIONALE

In the interdependent and hyperconnected digital world, cybersecurity resilience is essential for continuous existence and competitive advantage (Annarelli, Nonino & Palombi, 2020). The performance of CI (e.g. water supply systems) has traditionally been analysed using conventional risk assessment methods for their safe and reliable operation (Linkov & Trump, 2019). This approach allows responding adequately to known threats and hazards (Gasser et al., 2019). However, it has more recently become apparent that additional considerations and efforts are needed beyond the well-established risk-based techniques to ensure efficient recovery from disruptive events (Panteli & Mancarella, 2015).

As a result, increased attention has now shifted towards resilience of CI, which is considered fundamental to adequately addressing natural and human-origin disruptive events (Jackson, 2015). It is against this backdrop that a whole-systems approach is required to assess resilience of the water and wastewater CI against cyberthreats. This is crucial as security is

managed mostly in its own silo, with standards, governing bodies, policies and guideline documents geared specifically to a single area of security concern (DiMase, Collier, Heffner & Linkov, 2015).

AIM AND OBJECTIVES

The aim of the WP2 study was to evaluate the cybersecurity resilience of water CI in South Africa and provide recommendations for continuous improvement. The objectives of the study were as follows:

- Develop a socio-technical systems cybersecurity resilience assessment model.
- Evaluate the level of water sector CI cybersecurity resilience of South Africa.

METHODOLOGY

As the aim of the study was to perform a cybersecurity resilience evaluation of water CI, a suitable assessment model was required. To develop the cybersecurity resilience assessment model, two premises were made. The first premise was based on the socio-technical systems cybersecurity optimisation process developed by Malatji, Marnewick and Von Solms (2020), and validated by industry practitioners. The second premise was based on the modified National Institute for Standards and Technology (NIST) cybersecurity framework for CI protection – CI cybersecurity capability framework. The NIST cybersecurity framework is a best practice set of security guidelines used worldwide. The CI cybersecurity capability framework is essentially the modified NIST cybersecurity framework (NIST CF) as developed by Malatji, Marnewick and Von Solms (2021). The two frameworks were merged to develop a CI cybersecurity resilience assessment framework model that provides a whole-systems perspective of analysis.

The cybersecurity resilience assessment model was subsequently utilised to assess the cybersecurity resilience level of the water and sanitation sector in South Africa. This was accomplished through four case studies of water CI owners and operators. The cybersecurity resilience assessment model measured four metrics: maturity, utilisation, effectiveness and comprehensiveness. The maturity and utilisation of cybersecurity practices were measured through data collected via a survey and the findings were extrapolated to the entire sector.

The effectiveness and comprehensiveness metrics were computed through data collected by way of interviews, and the findings are only applicable to the individual case study organisations. These were used not only to triangulate the survey results, but also to identify the socio-technical cybersecurity vulnerability areas of concern (i.e. those security measures

that emphasise one aspect of cybersecurity – usually technical – over other aspects – usually human factors and physical security – thereby exposing gaps, since a security chain is as strong as its weakest link). The findings are summarised next.

RESULTS AND DISCUSSION

The study results are summarised as follows:

- 37,5% of the case study organisations utilise a formal security standard, guideline, or framework.
- 37,5% of the case study organisations have a formal cybersecurity governance structure in place.

The overall finding based on the above indexes is that the cybersecurity resilience of South Africa's water sector is average. That is, its capability to prepare and plan for, absorb, rapidly recover from, and successfully evolve from any human-made and/or autonomous adverse conditions, stresses, attacks and/or compromises is average. In particular, the areas of concern that need immediate attention and improvement in both the enterprise IT and ICS environments are in the maturity and utilisation elements of the cybersecurity practices. This is consistent with the fact that only 37,5% of the case study organisations utilise a formal security standard, guideline, or framework to direct and control their cybersecurity activities and have a formal cybersecurity governance structure in place.

RECOMMENDATIONS

The findings gave rise to the following general and policy recommendations:

- Set up security operations centres at larger sector organisations.
- Adopt cybersecurity standards, guidelines and/or frameworks at organisational level.
- Commission specialised teams for enterprise IT security and ICS cybersecurity.
- Conduct mandatory annual cybersecurity resilience assessments in the sector.

CONCLUSIONS AND FUTURE RESEARCH

A socio-technical systems (STS) cybersecurity resilience assessment model, which is the first objective of the study, was achieved by combining the CI cybersecurity capability framework, which is essentially the modified NIST CF, and the STS cybersecurity optimisation process. The STS cybersecurity optimisation process overarches the core of the cybersecurity resilience assessment model. This ensures that CI owners/operators do not emphasise only the technical cybersecurity safeguards at the expense of the other equally important non-technical security measures, thereby opening socio-technical cybersecurity vulnerability gaps. The second objective of the study, which was to evaluate the level of water sector CI

cybersecurity resilience of South Africa, was also achieved by deploying the STS cybersecurity resilience assessment model at selected water establishments. The case studies and model deployment in real-life settings also served as validation of the assessment model. Future research could deploy the assessment model with 50% or more of the water sector population/actors participating in the study. Future research could also explore how the data collection techniques of the assessment model could be improved to attain as near real-time data that reflects operational reality as possible.

KNOWLEDGE DISSEMINATION

The research conducted under WP2 has led to an international peer-reviewed journal publication. As a result, the content of this report is an outcome of the journal publication. In addition to the journal publication, the researchers were invited by the World Meteorological Organization (WMO) to be part of a panel discussion on 'The state of cyber security of water infrastructure in Africa'. The journal publication and the online link of the WMO webinar and associated report are as follows:

- Malatji, M., Marnewick, A. L. & Von Solms, S. (2021). Cybersecurity capabilities for critical infrastructure resilience. *Information and Computer Security*, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/ICS-06-2021-0091
- WMO. (2021). Water and cyber security – Protection of critical water related infrastructure – Part II (Online). Available at: https://web.archive.org/web/20210430092204/https:/public.wmo.int/en/events/meetings/water-and-cyber-security-protection-of-critical-water-related-infrastructure-part-ii (accessed on 01 July 2021).

ACKNOWLEDGEMENTS

The authors would like to thank the following individuals for their input during WRC Project C2021-2023-00354.

Name	Title	Affiliation
Dr Nonhlanhla Kalebaila	Research Manager	Water Research Commission
Ms Charmaine Khanyile	Project Co-ordinator	Water Research Commission
Mr Dumisani Gubuza	Reference group member	City of Tshwane
Ms Kgaogelo Kubyana	Reference group member	eMalahleni municipality
Mr Vusi Kubheka	Reference group member	RandWater
Ms Nomazwi Mhloma	Reference group member	eThekwini Metro municipality
Mr Mluleki Mnguni	Reference group member	Umgeni Water
Mr Moloko Monyepao	Reference group member	Ekurhuleni municipality
Mr Dan Naidoo	Reference group member	Umgeni Water
Dr Kiru Pillay	Reference group member	Department of Communication and Digital Technologies
Dr Renier van Heerden	Reference group member	SANREN
Dr Brett Van Niekerk	Reference group member	Durban University of Technology

This page was intentionally left blank

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS AND ABBREVIATIONS

AI	Artificial intelligence
CERT-RMM	Computer Emergency Response Team – Resilience Management Model
CI	Critical infrastructure
CISA	Cybersecurity and Infrastructure Security Agency
COBIT	Control Objectives for Information and Related Technologies
CSIRT	Cyber Security Incidents Response Team
HMI	Human-machine interface
ICS	Industrial control systems
ISO/TC	International Standardisation Organisation/Technical Committee
IT	Information technology
JO	Joint optimisation
LIMS	Laboratory information management system
Max	Maximum
MI	Maturity
Min	Minimum
N/A	Not applicable
NCPF	National Cybersecurity Policy Framework
NCSC	National Cyber Security Centre
NIST	National Institute for Standards and Technology
OT	Operational technologies
RMM	Resilience Management Model
SCADA	Supervisory control and data acquisition
SOC	Security operations centre
STS	Socio-technical systems
STS CAM	Socio-Technical Systems Cyberresilience Assessment Model
UI	Utilisation
USA	United States of America
WP	Work package
WSP	Water services provider

1. INTRODUCTION AND OBJECTIVES

1.1 Introduction

Resilience renders a more promising approach in the cybersecurity field to attain a comprehensive understanding of how systems can be impacted by adverse cyber events and how to recover from them (Gasser et al., 2019). Industry, governments and academia have all come to accept that it is highly unlikely, if not impossible, for all CI risks to be successfully identified and addressed (Chaves, Rice, Dunlap, & Pecarina, 2017; Clédel, Cuppens, Cuppens, & Dagnas, 2020). This is demonstrated by the recent cyberattacks on critical and non-critical infrastructure systems in the United States of America (USA).

New techniques are therefore needed to enable mitigation, adaptation and recovery from inevitable disruptions and cyberattacks on critical and interdependent infrastructure systems (DiMase et al., 2015; Ganin et al., 2017). Resilience has emerged from this realisation that not all threats and adverse events can be averted through risk assessment methods (Gasser et al., 2019). Thus, resilience is an attempt to overcome the limitations of traditional risk management methods in the cybersecurity of CI (Björck, Henkel, Stirna, & Zdravkovic, 2015; Carías, Arrizabalaga, Labaka, & Hernantes, 2020; Linkov & Kott, 2019). As the ability to prepare for and adapt to dynamic conditions and absorb and recover quickly from adverse events, resilience is the fundamental goal of the protection of CI (Roege et al., 2017). It is primarily concerned with the availability of mission critical systems and services with limited disruptions (Young & Leveson, 2014). Therefore, resilience is fundamentally about a system's intrinsic ability to adapt to unexpected events (Annarelli et al., 2020; Mohebbi et al., 2020), and does not emphasise the events themselves (Clédel et al., 2020).

The events and associated negative impacts are the fundamental concern of risk management (Heinimann & Hatfield, 2017). Thus, risk assessments provide for diagnostics and situation awareness capabilities (Hardison, 2018), whereas resilience is about the mitigation of unexpected disruptions (Arghandeh, Von Meier, Mehrmanesh, & Mili, 2016). It is the ability to recover quickly and the capacity to adapt in the face of challenging circumstances while maintaining critical services that distinguish resilient systems. Resilience techniques are therefore complementary to, but different from, those of risk management (Rieger, 2014). This is because resilience is essential when there is not enough historical data to calculate risk (Linkov & Trump, 2019; Roege et al., 2017).

Another distinguishing factor is that the scope of resilience-based, as opposed to risk-based, measurement methods is comprehensive and difficult to execute as it is an integrated life cycle approach involving key stakeholders across all business functions on-premises and in the cloud (Dickson & Goodwin, 2020). The difficulty in execution stems from the fact that

cyberresilience comprises numerous domains, e.g. information security, governance and business continuity, with hundreds of procedures within them and complex relationships between the domains and procedures (Carías, Labaka, Sarriegi, & Hernantes, 2019). Moreover, resilience measurements can be event-specific, framework-based, fuzzy, quantitative deterministic and/or probabilistic, or even qualitative (Gasser et al., 2019; Linkov & Kott, 2019; Thorisson, Lambert, Cardenas, & Linkov, 2017).

In terms of framework-based resilience measurements, a number of cyberresilience assessment guidelines, models and best practices have been proposed over the years (Clédel et al., 2020; Collier et al., 2014; Collier, Panwar, Ganin, Kott, & Linkov, 2016). However, due to a lack of standardised resilience metrics and diversity of opinions on how to attain good cyberresilience, a number of resilience assessment frameworks, standards and guidelines have been proposed (Mohebbi et al., 2020; Roege et al., 2017). Some of the diverse cyberresilience assessment frameworks, standards and guidelines include:

- International Standardisation Organisation/Technical Committee (ISO/TC) 292 security and resilience (ISO, 2021; Naden, 2021).
- The Resilience Matrix (Linkov et al., 2013).
- The Computer Emergency Response Team-Resilience Management Model (CERT-RMM) (Caralli et al., 2016; Roege et al., 2017).
- The MITRE corporation's set of cyberresilience assessment guidelines (Carías et al., 2020).
- Cyberresilience review (Roege et al., 2017).
- ISO 31000 as adapted for resilience assessments (Heinimann & Hatfield, 2017).
- ISO 27001 as adapted for resilience assessments (Annarelli et al., 2020).

Apart from the framework-based cyberresilience assessment methods mentioned above, many other studies have proposed different methods to assess the resilience of CI. These studies have also brought numerous new findings pertaining to the quantification of CI resilience (Rehak, Senovsky, Hromada, & Lovecek, 2019). However, most of the current cyberresilience frameworks, including the NIST CF, do not explicitly present the complex interdependent relationships between the different cyberresilience domains from an STS perspective.

The STS approach helps identify and address not only the technological, but also social and environmental cybersecurity threats and vulnerabilities (Malatji et al., 2020). This approach also ensures that the economic aspect is interwoven with the social and environmental aspects to achieve sustainability. Although the resilience matrix – physical, information, cognitive and social – by Linkov et al. (2013) addresses some of the STS dimensions, the

NIST CF comes the closest to addressing the cybersecurity resilience challenges from an STS perspective. However, it does not outline how the STS cybersecurity resilience assessments should be incorporated and operationalised. This forms part of the central aim of the study, as outlined next.

1.2 Project aim and objectives

The aim of WP2's study was to develop an STS cybersecurity resilience assessment model based on the five elements of the NIST CF and to determine the cybersecurity resilience levels of South Africa's water CI. The objectives of the study were as follows:

- Develop an STS cybersecurity resilience assessment model.
- Conduct case studies to determine the level of cybersecurity resilience at South Africa's water utilities.

1.3 Report layout

The report is structured as follows:

- The aim and objectives of this deliverable (WP2) are introduced in Section 1.
- The cybersecurity resilience literature is reviewed and discussed in Section 2 to gain insight into best resilience assessment practices. This is in relation to the first objective of the study.
- In Section 3, the study method employed to develop the cybersecurity resilience assessment model is outlined. Best cybersecurity resilience assessment practices are adopted in this section to develop an assessment model for the water sector of South Africa. This is in relation to the second objective of the study.
- In Section 4 the cybersecurity resilience assessment model is deployed in real-life settings in the form of case studies. Through the case studies, cybersecurity resilience levels of four water entities are assessed.
- Section 5 covers the validation of the cybersecurity resilience assessment model, as well as the case study findings.
- Recommendations pertaining to the water sector's cybersecurity resilience level are made in Section 6.
- Section 7 concludes the report and future focus areas for research are proposed.

2. CYBERSECURITY RESILIENCE

2.1 Introduction

Traditional risk management techniques to adequately defend against emerging cyberthreats are proving ineffective (Dickson & Goodwin, 2020) due to digital transformation initiatives including cloud computing, artificial intelligence (AI) and the (industrial) Internet of Things (Lees, Crawford, & Jansen, 2018; Tonhauser & Ristvej, 2019). Focused mainly on planning for continuity of operations in the event of system outages and failures, classical business continuity techniques should also evolve to include cyberthreats (Dickson & Goodwin, 2020). The incorporation of resilience, risk management, business continuity and practices from several other domains into the cybersecurity domain has created a discipline dedicated to improving cyber response capabilities such as incident detection, recovery and continual process improvement (Carías et al., 2020; Dickson & Goodwin, 2020). This has resulted in various definitions of resilience depending on the domain of application (Imani & Hajializadeh, 2020).

2.2 Cyberresilience definition

Sifting through the resilience literature highlights a lack of consensus on the definition of cybersecurity resilience across several domains (Imani & Hajializadeh, 2020). How resilience is defined depends heavily on each research domain (Gasser et al., 2019). Despite the lack of consensus, there is a common theme to the definition of resilience across all domains, i.e. the ability to minimise the magnitude and/or duration of adverse conditions and a system's inherent/design ability to absorb, adapt and recover from the negative conditions (Ayyub, 2014; Björck et al., 2015; Bodeau & Graubart, 2017; Clédel et al., 2020; Dessavreand & Ramirez-Marquez, 2015; Hale & Heijer, 2006; Linkov & Kott, 2019; National Academy of Sciences, 2012). Derived from the common themes across several domains, in this study resilience refers to:

> *the ability of critical infrastructure systems to prepare and plan for (anticipate), absorb (withstand), rapidly recover from (restore critical services) and successfully evolve from (adapt to) natural, human-made and autonomous adverse conditions, stresses, attacks and/or compromises.*

The resilience definition above takes on a meaning that encompasses the overall CI function (critical services of entire system) as the objective of resilience (Mohebbi et al., 2020). It is important to highlight this because in this study cybersecurity resilience, or simply cyberresilience, considers the state of a CI function following adverse conditions, stresses,

attacks and/or compromises on the underlying cyberinfrastructure. In other words, the study looks at the entire CI resilience, but only because of cybersecurity breaches.

2.3 Cyberresilience approach

As used in CI sectors, ICS have been designed for functionality, safety and performance – through reliability, availability and maintainability (Franciosi, Voisin, Miranda, Riemma, & Iung, 2020) – but not with security in mind (Campbell, 2016; Clark & Hakim, 2014). The legacy designs only considered unexpected but accidental hazards such as natural and adverse weather conditions, as well as human error (Clédel et al., 2020). Security and resilience, in addition to risk management, are considered complementary components of cybersecurity (Roege et al., 2017). Improving a system's resilience thus renders significant advantages in managing risk (Haimes, 2009).

2.3.1 Limitations of risk management on CI protection

Traditional risk management techniques begin with risk evaluations of known threats based primarily on historical data utilising the triplet approach: what can go wrong (threats), how likely is it to happen (vulnerabilities) and what is the impact (consequences) (Clédel et al., 2020; Collier et al., 2014; Gasser et al., 2019; Heinimann & Hatfield, 2017; Roege et al., 2017)? As already stated, the absence of historical and/or forecast data makes it prohibitively challenging to conduct a risk assessment that adequately accounts for the potential cascading impact of events on highly complex and interconnected CI (Linkov & Kott, 2019). Probabilistic risk-based techniques are therefore limited when it comes to strategies required to address the various types of threats and vulnerabilities on highly complex and interconnected CI (DiMase et al., 2015; Ganin et al., 2017).

To fill in the historical and/or forecast data gaps for probabilistic risk assessments, semi-quantitative techniques can be utilised by way of expert judgements (DiMase et al., 2015; Roege et al., 2017). This is where (cyber)resilience comes in. (Cyber)resilience is more concerned with a CI's adaptive capacity (Redman, 2014) to respond to (cyber)threats pre-, during and post-event for continuity of mission critical services (Annarelli et al., 2020; Roege et al., 2017; Young & Leveson, 2014). Resilience techniques have been shown to be more appropriate for this type of comprehensive scope of threat analysis than risk management techniques (Carías et al., 2020; Heinimann & Hatfield, 2017). Thus, resilience is essential when risk is incomputable as is the case in trying to quantify CI threats (Ganin et al., 2017; Linkov & Kott, 2019).

As shown in Figure 1, the importance of cyberresilience does not imply that risk management techniques should be completely discarded. If anything, organisations looking to improve their cybersecurity postures are better positioned to achieve this goal through risk assessments for informed decision making and continuous improvements (Hardison, 2018).

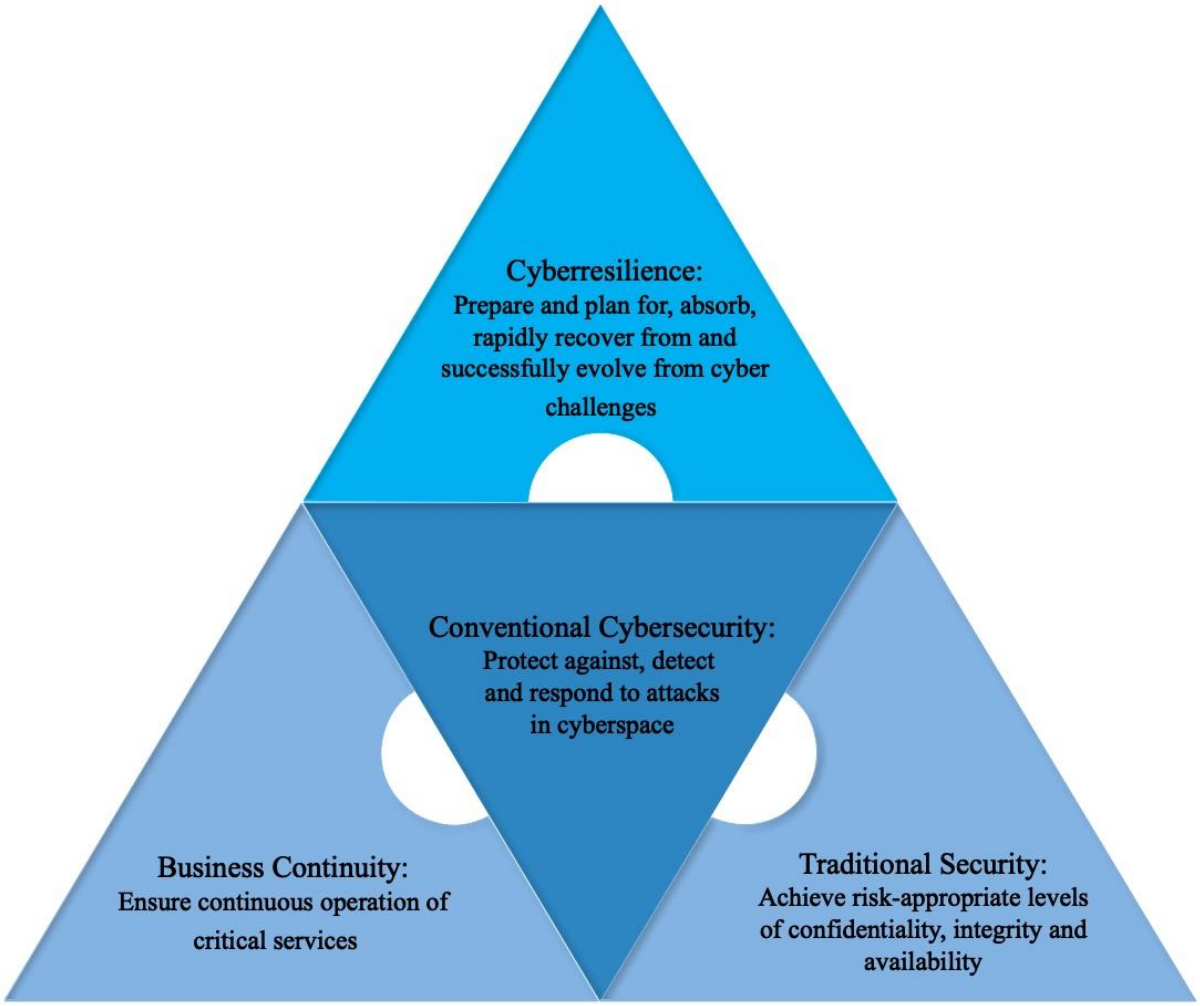

Figure 1. Cyberresilience as a component of cybersecurity

As shown in Figure 1, cyberresilience strategies assume that business continuity practices, which are usually risk-based, traditional security and cybersecurity are already in place (Bodeau, Graubart, Heinbockel, & Laderman, 2015). The notion is that cyberresilience capacities of an organisation complement these conventional practices as they have limited effectiveness against advanced persistent threats (Bodeau et al., 2015; Gasser et al., 2019; Linkov et al., 2013; Roege et al., 2017). As discussed in the next section, CI cyberresilience strategies are explored for their integrated approaches that recognise the interrelationships between people, business processes and technology ecosystems within and outside an organisation (Lees et al., 2018; Roege et al., 2017).

2.3.2 Cyberresilience capacities

Cyberresilience strategies are generally operationalised through four system resilience capacities (Hausken, 2020; Mohebbi et al., 2020). As shown in Figure 2, these are the preparedness, absorbability, restorability and adaptability capacities (Butler et al., 2014; Clédel et al., 2020; Francis & Bekera, 2014; Hausken, 2020; Linkov et al., 2013; Mohebbi et al., 2020).

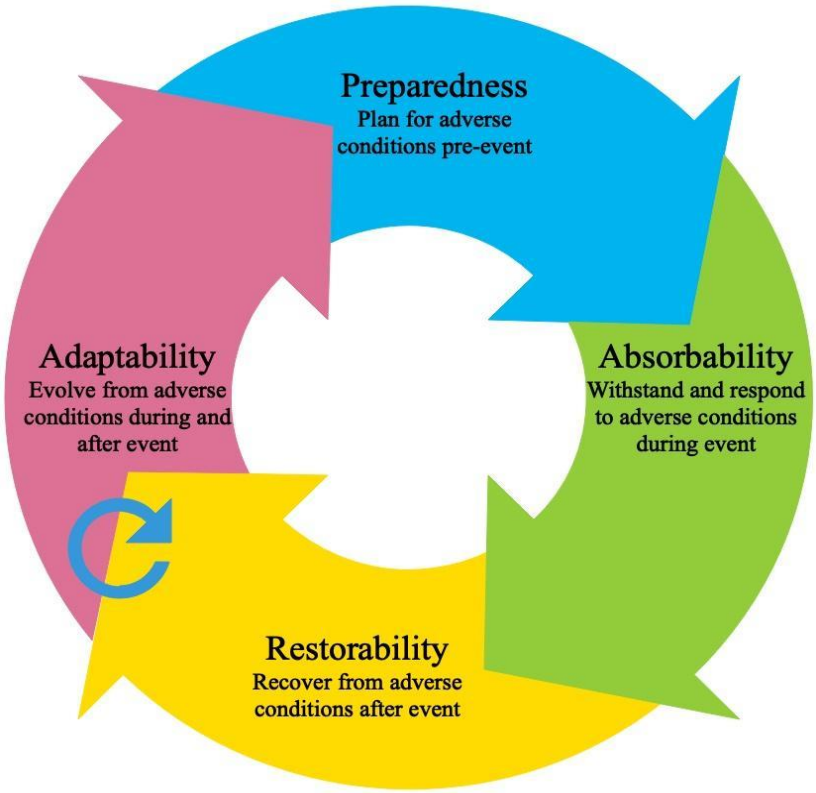

Figure 2. CI cyberresilience capacities

The four CI cyberresilience capacities are implied in the definition of cyberresilience provided earlier in section 2.2. Prior to an adverse condition, stress, attack and/or compromise, operationalisation of the first cyberresilience capacity – preparedness – should focus on preparing and planning for known and unknown, expected and unexpected threats (Babiceanu & Seker, 2019; Clédel et al., 2020). Once CI cyber protective and cyber defensive mechanisms have been breached (Roege et al., 2017), the second cyberresilience capacity – absorbability – focuses on local impacts to identify and protect critical system components that are more vulnerable to exploitation (Mohebbi et al., 2020). Absorbability speaks to the degree to which CI systems can withstand and minimise impacts from adverse conditions, stresses, attacks and/or compromises (Vugrin, Warren, & Ehlen, 2011).

The third capacity of CI cyberresilience – restorability – focuses on the ability to quickly recover and restore critical services to as close to their original state as possible (Vugrin et al., 2011). The fourth CI cyberresilience capacity – adaptability – focuses on the ability to more rapidly adjust to new and sometimes adverse conditions, stresses, attacks and/or compromises (Francis & Bekera, 2014; National Academy of Sciences, 2012; Ouyang, Dueñas-Osorio, & Min, 2012). The authors acknowledge that there are different schools of thought as to which comes first between restorability and adaptability. In this study, adaptability is considered to occur concurrently through the respond and recover activities. This is signified by the circular arrow between restorability and adaptability in Figure 2. Adaptability is therefore considered to start during the event in the absorbability capacity where CI systems need to quickly adjust to new and sometimes adverse conditions, stresses, attacks and/or compromises for the organisation to respond appropriately. The adaptability capacity ends after the event and during the restorability capacity activities.

As depicted by the circular arrow in Figure 2, it is an iterative process between restorability and adaptability for continuous adjustment to new conditions until all CI services are restored. Similarly, the arrows in each of the four CI cyberresilience capacities indicate that cyberresilience techniques can also be considered iterative. According to Rehak and Hromada (2018), the iterative nature of the cyberresilience strategies ensures continuous improvement of CI cyberresilience capacities for threat prevention, absorption, adaptation and recovery. If not continuously improved through assessments, cyberresilience strategies can become ineffective against certain adverse conditions, stresses, attacks and/or compromises (Hale & Heijer, 2006).

2.4 Cyberresilience assessment metrics

As stated in the introduction section, CI resilience metrics can be event-specific, framework-based, fuzzy, quantitative deterministic and/or probabilistic, or qualitative (Gasser et al., 2019; Linkov & Kott, 2019; Thorisson et al., 2017). In this study framework-based metrics were utilised for assessing and analysing system resilience (Clédel et al., 2020; Nan & Sansavini, 2017; Roege et al., 2017). A review of some of the cyberresilience frameworks is shown in Table 1. As already alluded to in the introduction section, STS gaps (last column) in Table 1 refer to a scenario where either the social, technical, or environmental dimension is emphasised more than the others, thereby opening vulnerabilities on the less emphasised ones. Still on the last column of Table 1, the term ‘classified’ means that security controls have been categorised along the social, technical and environmental dimensions, whereas ‘optimised’ means security controls categorisation is well balanced along the social, technical and environmental dimensions.

Table 1. Cyberresilience assessment frameworks

Framework	Source	Framework elements	STS gaps
Cyber resilience review	Cybersecurity and Infrastructure Security Agency (CISA) (2020)	Incomplete; Performed; Planned; Managed; Measured; Defined	Fundamentally technical and does not describe how security controls can be STS classified and optimised to identify socio-technical vulnerability gaps
Critical infrastructure elements resilience assessment	Rehak et al. (2019)	Robustness; Recoverability; Adaptability	Procedure for assessing the resilience of CI elements does not describe how security controls can be STS classified and optimised
Cybersecurity resilience maturity measurement	Mbanaso, Abrahams, & Apene (2019)	Identify; Protect; Detect Respond; Recover	Similar to NIST CF, framework does not describe how security controls can be STS classified and optimised
Seven pillars of cyberresilience	Carayannis et al. (2019)	Patient; Persistent; Persevering; Proactive; Predictive; Preventive; Pre-emptive	Maps its seven elements to the NIST CF functions but does not describe how security controls can be STS classified and optimised
Cornerstones of cyber resilient ICS	Lees et al. (2018)	Training; Policies and procedures; Host-based controls; Network-based controls; Risk management; Project management	Fundamentally generic and leans more towards technical measures; the guidelines do not describe how security controls can be STS classified and optimised
ICS cyber resilience assessment model	Haque et al. (2018)	Physical; Organisational; Technical	Environmental dimension is not explicit; framework does not describe how security controls can be STS classified and optimised
NIST CF	NIST (2018)	Identify; Protect; Detect; Respond; Recover	A comprehensive framework containing all three STS dimensions; does not describe how security controls can be STS classified and optimised to identify socio-technical vulnerability gaps
Resilience management framework	Heinimann & Hatfield (2017)	Establish context; Identify disruptions; Analyse resilience; Evaluate resilience; Build resilience	Based on the ISO 31000 standard and does not describe how security controls can be STS classified and optimised
CERT-RMM	Caralli et al. (2016)	Engineering; Enterprise management; Operations management; Process management	Does not describe how security controls can be STS classified and optimised
Cyber physical systems security framework	DiMase et al. (2015)	Policy and guidance; Governing bodies; Areas of concern; Cross-cutting capabilities	Does not describe how security controls can be STS classified and optimised
Cyber resiliency engineering framework	Bodeau & Graubart (2013)	Understand; Prepare; Prevent; Continue; Constrain; Reconstitute Transform; Re-Architect	Does not describe how security controls can be STS classified and optimised
Resilience matrix	Linkov et al. (2013)	Physical; Information; Cognitive; Social	Does not describe how security controls can be STS classified and optimised
National Cyber Security Centre (NCSC) cyber assessment framework	NCSC (2020)	Managing security risk; Protecting against cyberattack; Detecting cybersecurity events; Minimising the impact of cybersecurity incidents	Does not describe how security controls can be STS classified and optimised to identify socio-technical vulnerability gaps

Framework elements in the third column of Table 1 refer to the essential components of each framework for cyberresilience assessment. The diversity of the elements indicates a lack of consensus on resilience metrics, as previously highlighted by Mohebbi et al. (2020) and Roege et al. (2017). Bodeau and Graubart (2016), however, argue that no single cyberresilience metric or set of metrics is possible across all CI systems. Metrics should be customised according to stakeholder needs or to a specific system and/or mission (Roege et al., 2017).

A detailed review of the recommended cyberresilience assessment practices underpinning each framework element in Table 1 indicates that most of the frameworks do contain STS dimension attributes as defined by Davis, Challenger, Jayewardene and Clegg (2014) and Wu, Fookes, Pitchforth and Mengersen (2015), albeit not explicitly. However, close scrutiny of the practices reveals that the STS dimension attributes in the frameworks tend to lean more towards one or the other STS dimension, thereby creating socio-technical vulnerability gaps (Washington & Hacker, 2000). It is a classic case of the security chain is only as strong as its weakest link, as these gaps can be exploited by attackers.

Additionally, the frameworks in Table 1 do not outline how security controls can be classified into STS dimensions and optimised to identify socio-technical cybersecurity vulnerability gaps. This is crucial as, for example, a cyberresilience assessment that indicates a satisfactory level of technical measures could be misinterpreted as adequate security safeguards. In this scenario the CI would also be considered as resilient. However, this scenario could mean that the cybersecurity technical dimension is being emphasised more than the other, as Carayon et al. (2015) put it, equally important STS dimensions.

As the cornerstone of STS, joint optimisation (JO) should be determined to eliminate these kinds of false positives (Chen & Redar, 2014). JO refers to an STS technique concerned more with harnessing the best of both the technical and human aspects of organisational practices within a given environment (Carayon et al., 2015; Mumford, 2006). In other words, improving one aspect of an STS requires an improvement of the others to maintain the best possible performance (Carayon et al., 2015; Troyer, 2017; Walker et al., 2007). Therefore, to maintain the best possible cybersecurity performance in a CI, resilience assessments should consider a whole-systems perspective that can identify socio-technical cybersecurity vulnerability gaps (Hardison, 2018; Troyer, 2017). A framework-based STS cyberresilience assessment model is proposed by the authors to address the STS gap.

As a component of cybersecurity, cyberresilience comprises preparedness, absorbability, restorability and adaptability capacities. CI owners/operators must therefore ensure that their cyberinfrastructure can anticipate, withstand, rapidly recover from and successfully adapt to natural, human-made and autonomous adverse conditions, stresses, attacks and/or compromises. This can only be achieved through an integrated cyberresilience assessment model.

3. CYBERRESILIENCE ASSESSMENT MODEL

3.1 Introduction

The development of the socio-technical systems cyberresilience assessment model (STS CAM) as the cybersecurity resilience evaluation tool of the study was based on five elements of the NIST CF. These ensure that the four cyberresilience capacities are seamlessly integrated to determine the level of resilience of any CI, water CI included. To ensure that the cyberresilience assessment model was holistic and balanced, an STS approach was incorporated to overarch both the five NIST CF elements and four cyberresilience capacities. Operationalisation steps of the STS CAM are outlined in this section to ensure that the resilience assessment tool can be tested in real-life settings.

3.2 Resilience assessment model development

3.2.1 Model development approach

The STS CAM is underpinned by five NIST CF elements which, according to Hasan, Ali, Kurnia and Thurasamy (2021), are the following:

- *Identify*: Activities undertaken to pinpoint the cybersecurity risks an organisation may be exposed to.
- *Protect*: Activities undertaken to safeguard cyberinfrastructure and mission critical services.
- *Detect*: Activities undertaken to monitor anomalous network behaviour and identify the occurrence of cyber compromises.
- *Respond*: Activities undertaken to withstand and adapt to adverse conditions to defensively and/or offensively react to detected cyber compromises.
- *Recover*: Activities undertaken to restore mission critical services reduced or completely shut down due to cyber compromises.

To develop the STS CAM two premises were made and each was published as a separate study. The first premise was published by Malatji et al. (2021) as the utilities CI cybersecurity governance framework, or simply the CI cybersecurity capability framework. This framework is underpinned by five elements adopted from the NIST CF subdivided into 29 cybersecurity practices at level 3 (cybersecurity capability domains) and 140 cybersecurity practices at level 2 (cybersecurity capabilities) (Malatji et al., 2021). Figure 3 summarises the CI cybersecurity capability framework according to Malatji et al. (2021).

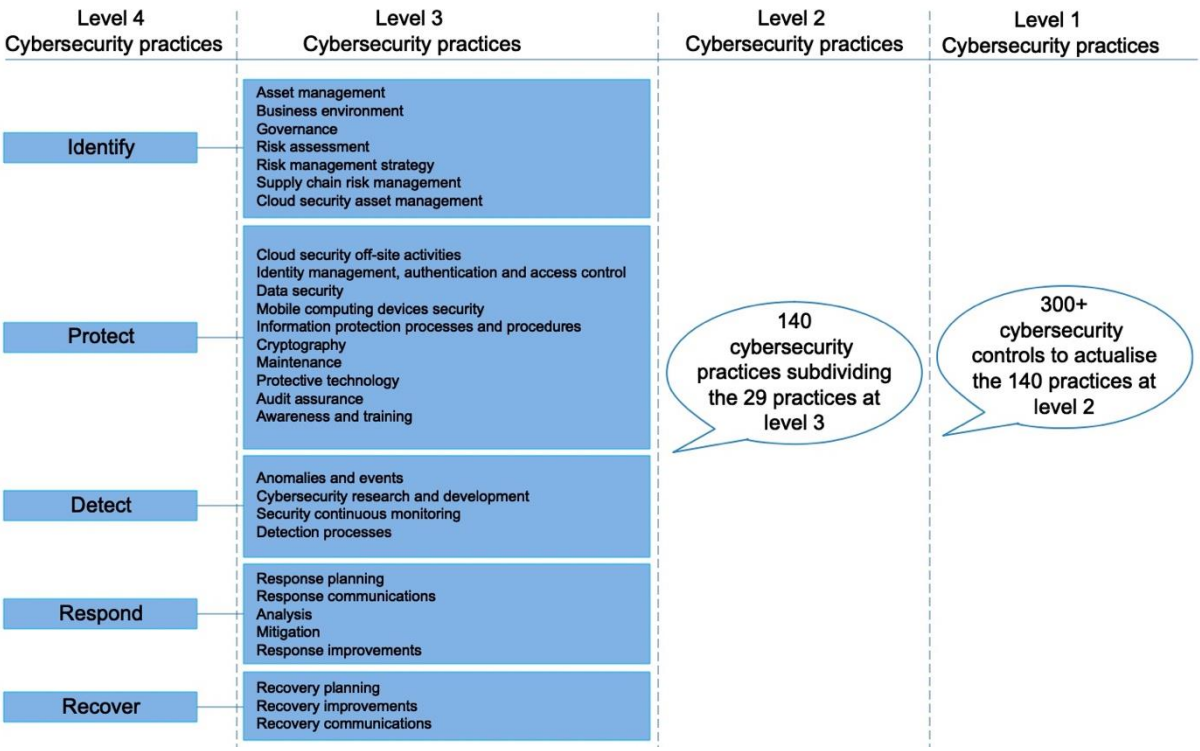

Figure 3. CI cybersecurity capability framework

The second premise is the STS cybersecurity optimisation process by Malatji et al. (2020). This study asserts that the enterprise systems security chain is only as strong as its weakest link between the social (including human factors), technical (technological cyber defences) and environmental dimensions. Figure 4 summarises the STS cybersecurity optimisation process according to Malatji et al. (2020). The STS cybersecurity optimisation process comprises three fundamental elements (Malatji et al., 2020):

- *Classify*: Activities undertaken to categorise cybersecurity controls into either of the three STS dimensions (social, technical and environmental) according to set STS criteria.
- *Optimise*: Activities undertaken to ensure that neither of the three STS dimensions is emphasised more than the others. If this happens, socio-technical cybersecurity vulnerabilities are likely to emerge as weak links to be exploited by attackers. This element is also known as joint optimisation (JO).
- *Mature*: Activities undertaken to monitor and continuously improve cybersecurity resilience practices through a capability maturity model.

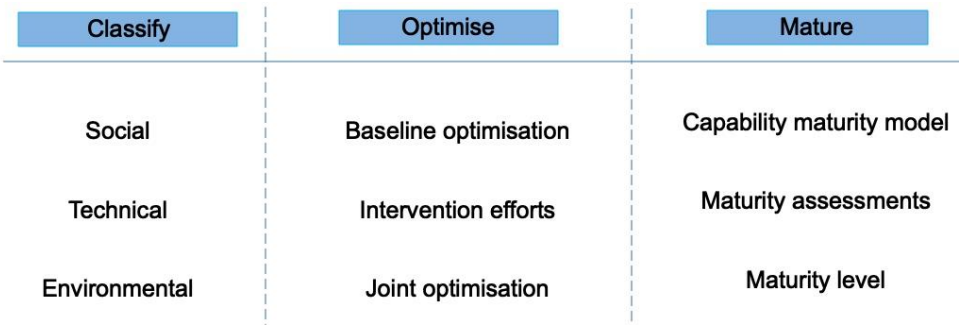

Figure 4. STS cybersecurity optimisation process

The proposed STS CAM comprises at its core the five elements of the CI cybersecurity capability framework. These are overarched by the three STS cybersecurity optimisation elements, after the five core elements are arranged according to the proactive and reactive cybersecurity strategies and grouped together into the four resilience capacities – *preparedness, absorbability, adaptability, restorability* – discussed in section 2.3.2 (see Figure 2). Figure 5 shows how the STS CAM was developed as the cybersecurity resilience assessment tool of the study.

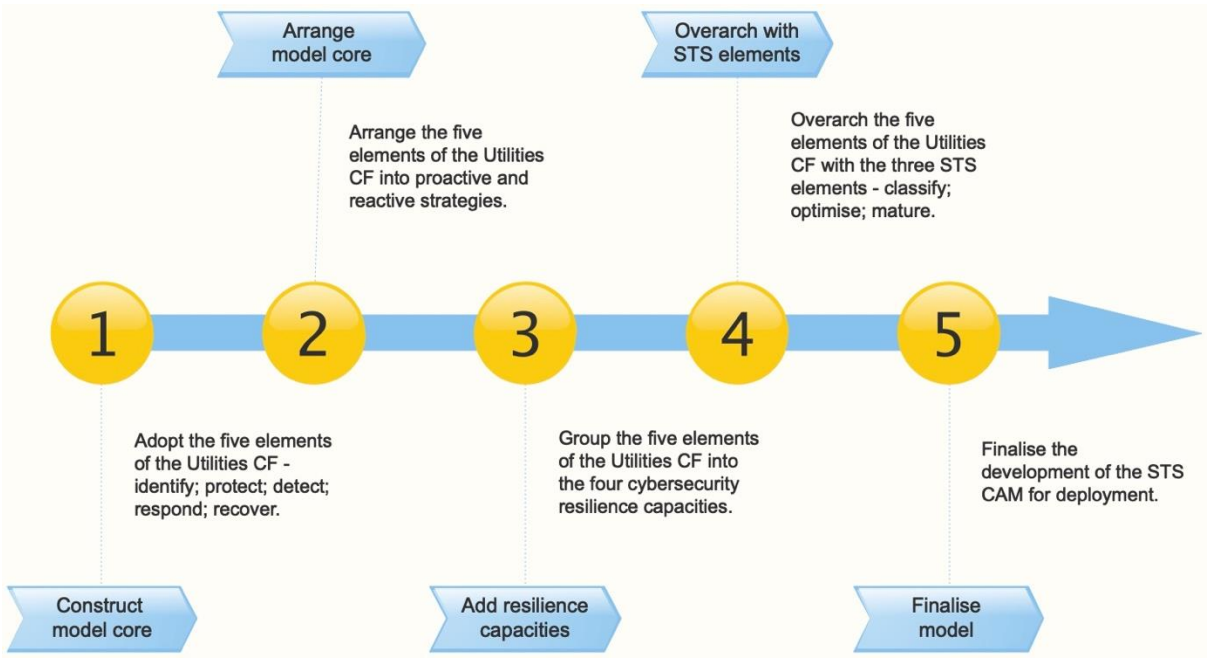

Figure 5. STS CAM development process

Thus, the STS CAM is an integration of Figures 3 and 4. Figure 5 summarises how this integration was achieved to yield a whole-systems cybersecurity resilience assessment model. The development of the model is discussed in the next section.

3.2.2 Model development

The development of the STS CAM utilised the five steps outlined in Figure 5 in the previous section. The first step was to construct the core of the model using the five elements of the CI cybersecurity capability framework in Figure 3. The second step was to arrange the five elements into proactive and reactive cybersecurity strategies. According to Pescatore (2020), the identify and protect elements can be considered as more proactive, and the detect, respond and recover elements as reactive. The third step was to group together the five elements into the four CI cybersecurity resilience capacities. The fourth step was to overarch the five elements of the CI cybersecurity capability framework with the three STS cybersecurity optimisation elements in Figure 4. Execution of these five model development steps results in the STS CAM shown in Figure 6.

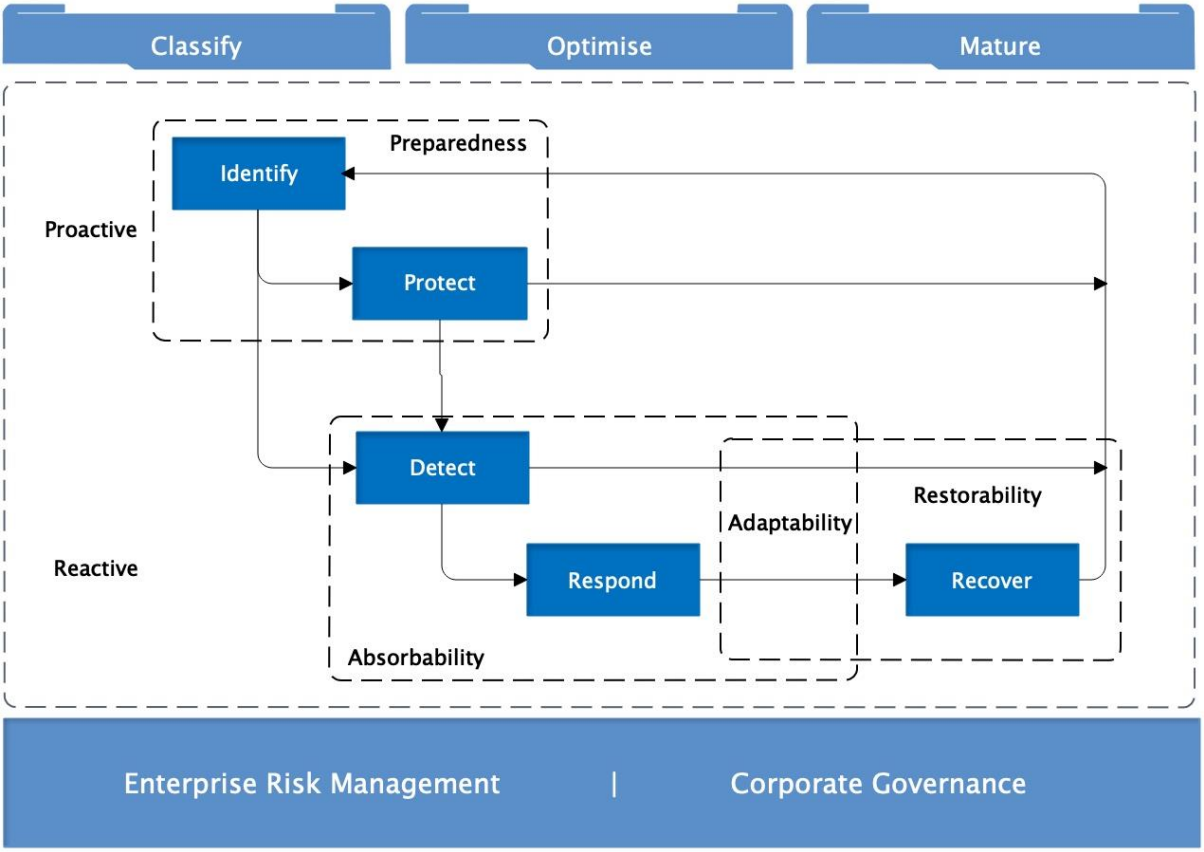

Figure 6. STS CAM

The STS CAM enables an integrated life cycle approach and is anchored by good enterprise risk management and corporate governance to provide a bridge between boards of directors and executive management (De Bruin & Von Solms, 2016; Susskind, 2014; WEF, 2020). The STS CAM can also serve a dual purpose of being both a cyberresilience assessment model and a holistic STS cyberresilience capability framework for the protection of cyberinfrastructure. The STS CAM is therefore referred to as a framework model. However,

the purpose of this study was to utilise the STS CAM only as an assessment tool to determine the level of resilience of water CI utilities in South Africa. In this regard, the STS CAM can be operationalised according to the process outlined in the next section.

3.3 Model application steps

The application of the STS CAM was carried out through case studies at four water entities located in different provinces of South Africa. The steps for operationalising the STS CAM are outlined in this section. The cybersecurity resilience case studies are discussed in detail in Section 4. The STS CAM operationalisation steps are based on the two premises adopted for the development of the model: 1) the five core elements of the model (identify; protect; detect; respond; recover); and 2) the three STS cybersecurity elements (classify; optimise; mature). Thus, the operationalisation steps are without regard to the notions of proactive/reactive and preparedness/absorbability/adaptability/restorability. These are used more for strategic reporting purposes as they have no influence whatsoever on the cybersecurity practices within the five core elements of the model and the three overarching STS cybersecurity elements. The application steps of the STS CAM are summarised in Figure 7.

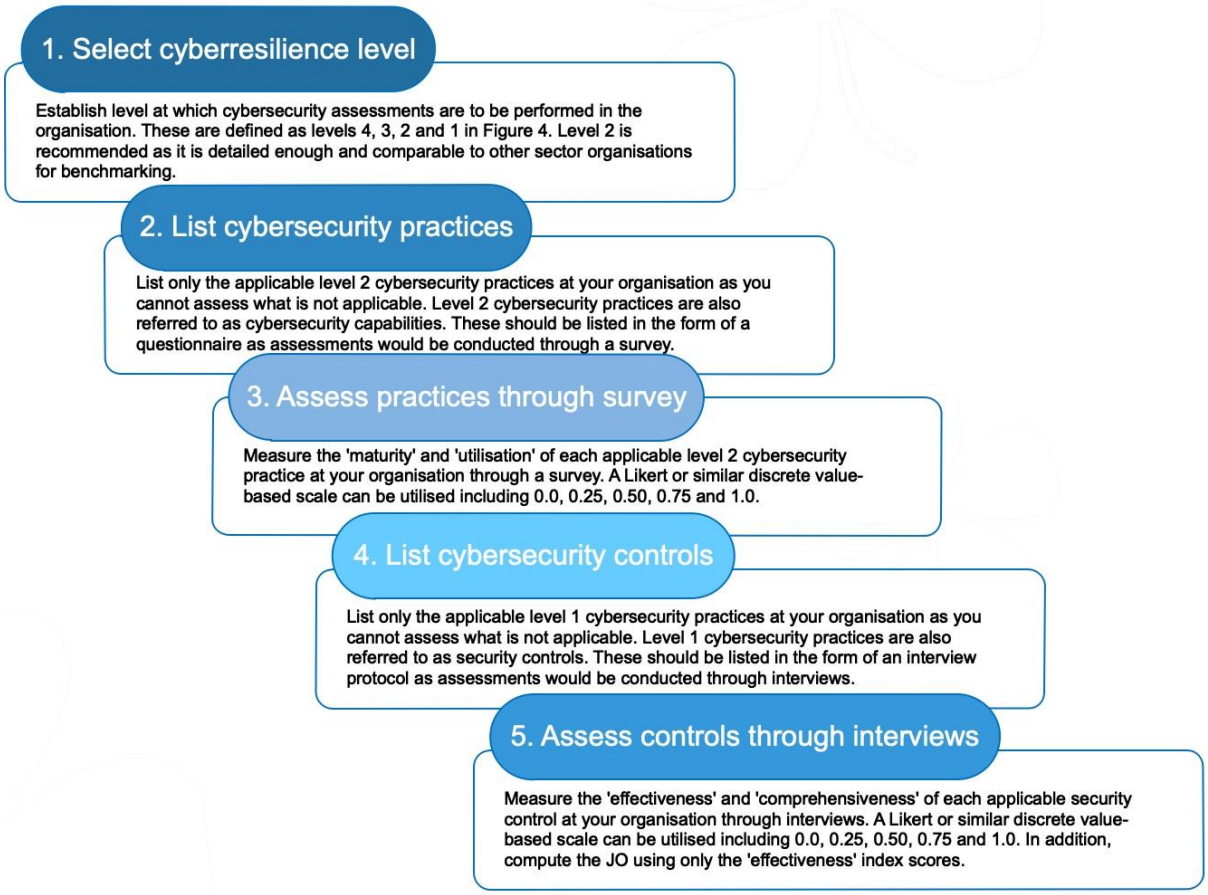

Figure 7. STS CAM application steps

As shown in Figure 7, the first step of applying the STS CAM is to establish the level at which cybersecurity assessments are to be performed in the organisation. These are defined as levels 4, 3, 2 (and 1) and can be summarised as follows (Malatji et al., 2021; Donaldson, Siegel, Williams, & Aslam, 2018):

- Level 4. Highest level of structure for organising desired cybersecurity outcomes. This is usually at enterprise level and is included in the enterprise risk management strategy.
- Level 3. Cybersecurity capability domains which are essentially security functional/focus areas to achieve desired cybersecurity outcomes.
- Level 2. Cybersecurity capabilities which are essentially competencies within each security functional area to achieve desired cybersecurity outcomes.
- Level 1. Cybersecurity controls to achieve desired cybersecurity outcomes.

The lower the level of resilience assessment, the more detail and level of effort required, and vice versa (Donaldson et al., 2018). This means that the more detailed an assessment exercise, the more resources and time are required. It is therefore at the discretion of the CI operators to determine which level of resilience assessment would be appropriate for each successive resilience evaluation. Whereas the cybersecurity capability domains determine the focus areas for achieving desired cybersecurity outcomes, the cybersecurity capabilities determine what (competencies) must be implemented in those focus areas to achieve desired cybersecurity outcomes (Malatji et al., 2021). Therefore, for individual organisations in a CI sector, the authors recommend that resilience assessments be conducted at level 2 (cybersecurity capabilities). Levels 4 and 3 are too high to provide any meaningful insights at organisational level. The other advantage is that level 2 resilience results can be extrapolated to the sector-wide level by aggregating the overall resilience scores per sector member organisation.

To drill down to the lowest level of under-performing areas of concern (Mbanaso, Abrahams, & Apene, 2019), the authors recommend that individual organisations within a CI sector conduct level 1 (security controls) resilience assessments using only the STS cybersecurity optimisation process (Malatji et al., 2020). Utilising only the STS cybersecurity optimisation process to conduct level 1 resilience assessments provides the required level of detail to gain meaningful insights. The STS cybersecurity optimisation process is only blended within the STS CAM to ensure that assessments conducted at levels 4, 3 and 2 are socio-technically appraised. This also serves as a form of triangulation, as the STS resilience assessment findings at level 1 should align with those at the higher levels. Thus, conducting resilience assessments at level 2 is only a recommendation when utilising the STS CAM for sector-wide resilience assessments.

As the second step of the STS CAM application, list all the cybersecurity capabilities (level 2 cybersecurity practices) in the form of a questionnaire, provided that the resilience assessment is being conducted at level 2 as recommended. It becomes apparent that conducting an assessment at level 2 automatically determines the resilience state at levels 3 and 4. However, the opposite (from 2 downwards, and even from 4 downwards) does not apply.

The third step is to determine the resilient indexes to be measured per cybersecurity capability. The authors recommend that the maturity and utilisation indexes be measured (Donaldson et al., 2018). The *maturity index* determines the degree to which organisational cybersecurity practices at level 2 have been formalised and optimised (i.e. how well and correctly a cybersecurity capability is implemented), and the *utilisation index* determines the consistency and extent to which organisational cybersecurity practices are being used (i.e. how consistently and correctly an implemented cybersecurity capability is practised) (Donaldson et al., 2018). It is important to measure both maturity and utilisation indexes. This is because an organisation can have all security controls present, correctly implemented and matured, but if they are not utilised, a persistent attacker will neutralise them (Donaldson et al., 2018). The opposite also applies. In other words, an organisation can religiously utilise all present security controls, but if they are not correctly implemented and matured, they can be ineffective.

To compute the maturity and utilisation indexes, a numerical scale is required. The overall cyberresilience maturity and utilisation indexes can be computed per CI sector organisation using the selected numerical scale. The results should be extrapolated to the sector-wide resilience and risk posture, and areas requiring immediate attention should be identified. The cybersecurity areas requiring immediate attention can only be identified if a minimum required level for both indexes has been defined. This is at the discretion of both individual organisations and their sector bodies, for example a water cybersecurity incidents response team (CSIRT). A formal workshop(s) or online survey can be utilised to collect the data from the questionnaire. The survey questionnaire is presented in Appendix A. Either way, the prepared questionnaire should be completed using expert judgement by the different stakeholders within the organisation. Both maturity and utilisation indexes can be computed as follows:

$$Index\ score = \frac{\sum O_n}{n} \quad (1)$$

where O denotes the object of measure (cybersecurity capability or level 2 security practice in this case) and n signifies the number of participants who allocated a score to the cybersecurity capability object of measure. Similarly, the overall resilience index (separate

for maturity and utilisation indexes) for the organisation would be the average of all the individual index scores.

Note that if all 140 capabilities were included in the survey questionnaire, 140 scores as calculated with equation (1) will roll up to 29 capability domain scores. The fourth step can occur in parallel with the third, or subsequently, as it also evaluates resilience, albeit at level 1 (security controls). There are two tiers to level 1 cyberresilience assessment. Tier 1 is the more detailed cyberresilience assessment using only the STS cybersecurity optimisation process (Malatji et al., 2020), as already mentioned. Conducting tier 1 resilience assessment at level 1 will also require a workshop or series of workshops with various stakeholders within and outside the enterprise. Tier 2 is less detailed and uses lean aspects of the STS cybersecurity optimisation process as contained in the STS CAM. Tier 2 is basically a light version of the full STS cybersecurity optimisation process and is recommended for use in conjunction with the STS CAM processes described above.

To operationalise tier 2 cyberresilience assessment at level 1, an interview protocol should be prepared. This protocol should contain only two questions. The first question should elicit enterprise IT and ICS cybersecurity controls data from the various stakeholders within the organisation. Quite simply, all the cybersecurity controls in the IT and ICS environments need to be listed. The second question seeks to determine the effectiveness and comprehensiveness scores of these cybersecurity controls. Effectiveness measures how efficient or effective the stakeholder thinks the cybersecurity control has been, and comprehensiveness measures how fully or comprehensively the stakeholder thinks the cybersecurity control is utilised in mitigating cyberrisks and protecting the organisation (Donaldson et al., 2018). Effectiveness and comprehensiveness indexes can also be computed using equation (1).

To identify the socio-technical cybersecurity gaps, the listed (IT and ICS) cybersecurity controls should be classified according to their social, technical and environmental dimensions (Malatji et al., 2020). Equation (2) can be used to compute socio-technical cybersecurity gaps (Malatji et al., 2020).

$$JO_{before} = \frac{Max\ (X_b,Y_b,Z_b) - Min\ (X_b,Y_b,Z_b)}{Average\ (X_b,Y_b,Z_b)} \quad (2)$$

where the aggregate effectiveness scores for cybersecurity controls classified as social are denoted by X_b, technical by Y_b and environmental by Z_b. The b subscript denotes resilience

assessments conducted before cybersecurity improvement intervention efforts (Malatji et al., 2020)*. JO is short for joint optimisation.*

JO refers to how optimised the organisational cybersecurity controls are, meaning that no single STS dimension is emphasised more than the others (Malatji et al., 2020). If this happens, socio-technical cybersecurity gaps are likely to emerge as weak links that can be exploited to establish a foothold in the organisation. The *Max* (X_b,Y_b,Z_b) variable refers to usage of only the highest score of the three STS dimensions and, likewise, *Min* (X_b,Y_b,Z_b) refers to usage of only the lowest score (Malatji et al., 2020). The *Average* (X_b,Y_b,Z_b) variable denotes the average score of the total number of aggregated effectiveness scores per cybersecurity control (Malatji et al., 2020). Equation (1) can be used to compute, individually, the aggregate effectiveness scores for the social X_b, technical Y_b and environmental Z_b dimension variables.

Once all the steps have been completed, the final activity to perform could be to compare the level 2 and level 1 areas of cyberresilience concern in the organisation based on the results. Although no perfect alignment is expected, as these are subjective expert judgement scores, there should nonetheless be no extreme deviations from the findings. Otherwise, the elicited data is not reliable and either fuzzy models should be applied to the data (Azadeh, Salehi, Arvan, & Dolatkhah, 2014; Clédel et al., 2020), or the assessment should be repeated using different methods, for example focus groups with all the key stakeholders in the organisation. Moreover, CI sector organisations should continually share cybersecurity incidents and resilience assessment information with the sector CSIRT as and when they become available. This is a requirement in South Africa as outlined in the roles and responsibilities of public sector CSIRT in the National Cybersecurity Policy Framework (NCPF) (South Africa, 2015).

Although this study focused specifically on resilience of the entire CI as a result of cyber adverse conditions, cyber stresses, cyberattacks and/or cyber compromises, the model itself can also be used to evaluate resilience to natural and adverse weather threats. The STS CAM was deployed at a public sector entity responsible for water and wastewater services. The (pilot) cyberresilience case study is discussed in the next section.

The STS CAM is an integrated resilience assessment model of the study and is based on the five elements of the CI cybersecurity capability framework. In addition, the STS CAM elements are arranged according to the four cyberresilience capacities to ensure that cybersecurity preparedness, absorption, adaptation and recovery activities are addressed. To make the STS

CAM more holistic, a socio-technical systems approach was incorporated in the design and development of the model.

4. ASSESSMENT OF CYBERRESILIENCE THROUGH CASE STUDIES

4.1 Introduction

Cyberinfrastructure resilience of four water CI operators was assessed using the STS CAM application steps outlined in the previous section. As shown in Figure 8, these assessments were conducted at level 2 (cybersecurity capabilities) as recommended by Malatji et al. (2021). A cyberresilience assessment questionnaire containing 140 questions based on 140 CI cybersecurity capabilities was developed. The capabilities were derived from the CI cybersecurity capability framework developed by Malatji et al. (2021). The survey questionnaire is presented in Appendix A. The assessments required the maturity and utilisation indexes to be computed for level 2 cybersecurity practices at all four case study organisations, as shown in Figure 8.

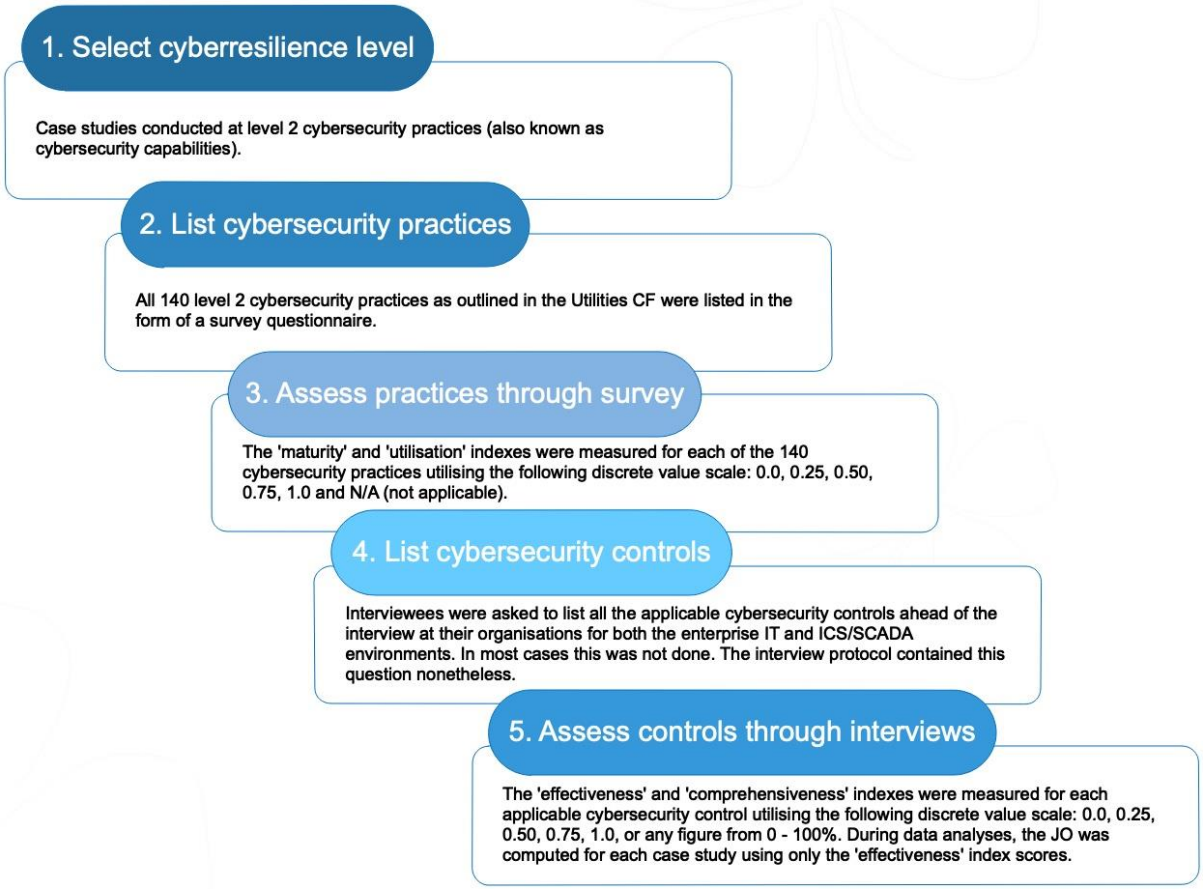

Figure 8. Case study approach

Virtual pre-survey workshops were held for each case study to explain the cyberresilience assessment questionnaire. This was to ensure consistent understanding of questions by all participants. A self-administered online survey link was subsequently sent to all participants, and the following discrete value scale was adopted in the survey for both the maturity and utilisation indexes:

- 0,000 (applicable but absent) – same as 0%.
- 0,250 (weak) – same as up to 25%, and more than 0%.
- 0,500 (good) – same as up to 50%, and more than 25%.
- 0,750 (very good) – same as up to 75%, and more than 50%.
- 1,000 (excellent) – same as up to 100%, and more than 75%.
- N/A (not applicable).

The interview protocol contained only four questions for all case studies. As shown in Figure 8, the first two questions sought to determine the types of cybersecurity controls used in both the IT and ICS environments, and the perceived effectiveness and comprehensiveness scores for those controls. The effectiveness and comprehensiveness indexes needed to be computed in the subsequent data analysis using equations (1) and (2). From these two questions the cybersecurity controls were *classified* into either the social, technical and environmental dimensions as described by Malatji et al. (2020).

Subsequently, the JO index to determine the socio-technical cybersecurity vulnerability gaps to *optimise* the controls was computed. The *mature* process activity of the STS cybersecurity optimisation process was not necessary as it is inherently contained within the overall resilience assessment exercise in the STS CAM. The first two questions are the only required interview questions for the operationalisation of the STS CAM to evaluate the effectiveness and comprehensiveness of organisational security controls.

The last two questions sought to establish the existence and configuration of the cybersecurity governance structure, if any, and the types of cybersecurity incidents experienced. These questions are not essential for the operationalisation of the STS CAM. They emanated from the pre-survey workshop of the first case study as follow-up questions for the interviews. These four questions were then kept the same for all four case studies. Unlike the survey questionnaire where the discrete value scale had fixed options to select from, interviewees could score the effectiveness and comprehensiveness of each cybersecurity control with any value from 0-100% (i.e. 0,000-1,000). The survey and interview results follow.

4.2 Case study 1

The first case study was a water services provider (WSP) headquartered in the Mpumalanga Province of South Africa. Four participants took part in the study – three from IT and one from the ICS environment. Together, the three IT participants were at tactical and operational levels and the ICS participant operated at both strategic and tactical levels.

4.2.1 Survey findings

On the survey closing date all three IT participants had completed the survey and the ICS participant had not. The water cyberresilience assessment results from the survey are shown in Table 2 below. As the assessment was conducted at level 2 cybersecurity practices (140 cybersecurity capabilities), the results in Table 2 have been rolled up to level 3 cybersecurity practices (29 cybersecurity capability domains).

Table 2. Case 1 survey results

Level 3 (Cybersecurity capability domain)	**Maturity**	**Utilisation**
Asset management	*0,292*	*0,222*
Business environment	*0,217*	*0,283*
Governance	*0,208*	*0,229*
Risk assessment	*0,292*	*0,319*
Risk management strategy	*0,361*	*0,333*
Supply chain risk management	*0,217*	*0,217*
Cloud security asset management	*0,250*	*0,250*
Cloud security off-site activities	*0,387*	*0,357*
Identity management, authentication and access control	*0,250*	*0,500*
Data security	*0,458*	*0,448*
Mobile computing devices security	*0,144*	*0,250*
Information protection processes and procedures	*0,406*	*0,399*
Cryptography	*0,083*	*0,083*
Maintenance	*0,375*	*0,375*
Protective technology	*0,367*	*0,367*
Audit assurance	*0,250*	*0,250*
Awareness and training	*0,333*	*0,333*
Anomalies and events	*0,350*	*0,367*
Cybersecurity research and development	*0,125*	*0,250*
Security continuous monitoring	*0,313*	*0,396*
Detection processes	*0,150*	*0,183*
Response planning	*0,167*	*0,167*
Response communications	*0,217*	*0,217*
Analysis	*0,267*	*0,283*
Mitigation	*0,139*	*0,194*
Response improvements	*0,313*	0,542
Recovery planning	*0,167*	*0,250*
Recovery improvements	*0,208*	*0,250*
Recovery communications	*0,167*	*0,167*
Overall	**0,258**	**0,292**

The same 29 cybersecurity capability domain results are presented as a spider graph or heat map in Figure 9 where MI represents maturity of the cybersecurity capability domain and UI denotes utilisation. The focus areas (domains) for achieving desired cybersecurity outcomes are visualised differently in Figure 10.

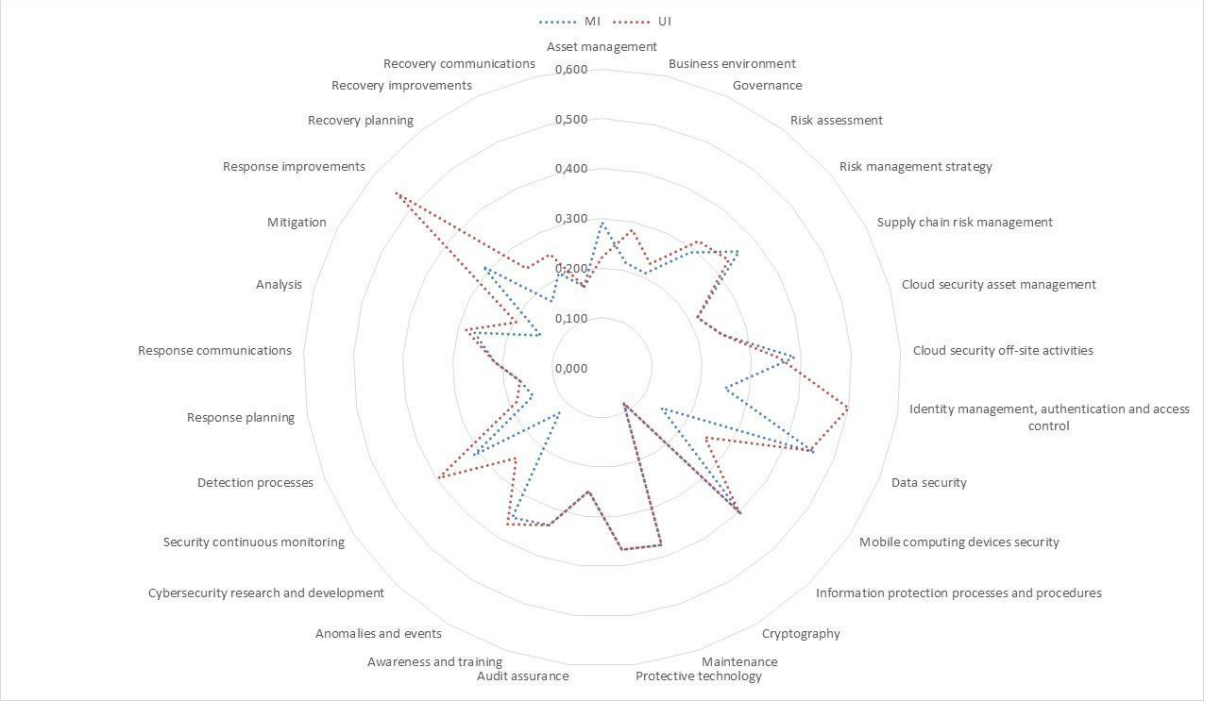

Figure 9. Spider graph visualisation of case 1 survey results

It can be seen from the italicised entries in Table 2 and Figure 9 that none of the cybersecurity capabilities received a maturity index score of 0,500 (good) or above. However, only two cybersecurity capabilities received a utilisation index of 0,500 (good) or above, namely:

- Identity management, authentication and access control
- Response improvements

This means that the participants believed that the WSP's utilisation of the enterprise IT approach to identifying, authenticating and authorising employees, vendors and other partners to access systems and physical assets was good. Likewise, the participants believed that the WSP's utilisation of IT security response activities against threats by incorporating lessons learnt from previous and current detection/response activities was also good. The data security capability domain scored just under 0,500 (good) in both the maturity and utilisation indexes. It can be motivated that the essential requirements for all the cybersecurity capability domains (level 3) would need to be 0,500 (good) for minimum cyberresilience operations. This can only be the case if subsequent cybersecurity capabilities (level 2) score maturity and utilisation indexes of at least 0,500 (good).

The recommended (international best practices) baseline level for cyberresilience operations is estimated to be about 0,750 (very good). However, each organisation must determine their own operational cyberresilience target based mainly on three aspects as recommended by NIST (2018): their security requirements, their business objectives and their technical

environment/abilities. These factors will inform the organisation on how to work from this baseline to set goals, such as to first obtain a 0,400 or 40% maturity, then 0,500 (50% maturity) and so on. When considering the two indexes separately, the maturity index was plotted against the recommended (international best practices) baseline level – 0,750 (very good) – and essential cybersecurity capability level – 0,500 (good). Figure 10 shows the maturity index graph with cyberresilience areas of concern for future improvements below the 0,500 (good) line.

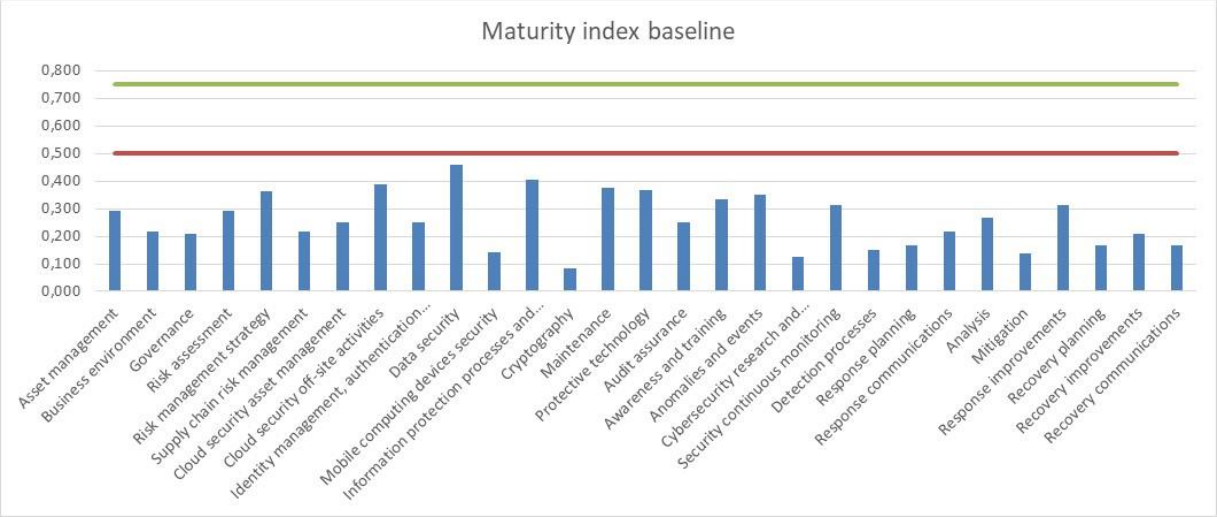

Figure 10. Case 1 maturity index graph

Similarly, the utilisation index was plotted against the same recommended variables as the maturity index. Figure 11 shows the utilisation index graph with cyberresilience areas of concern for future improvements below the 0,5 (good) line.

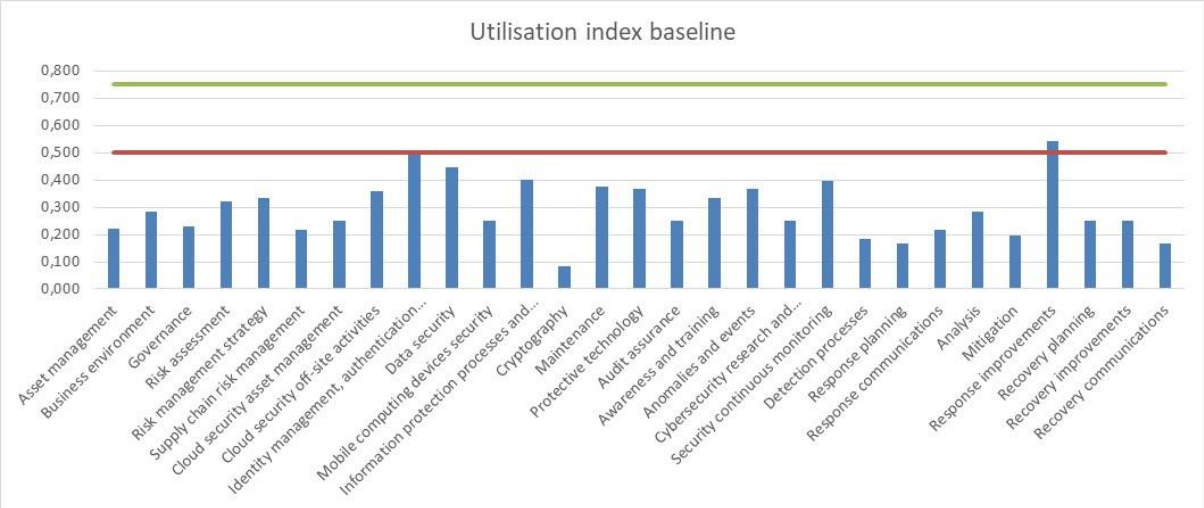

Figure 11. Case 1 utilisation index graph

It can be seen from the cyberresilience index graphs in Figures 10 and 11 that the study identifies the WSP cyberresilience areas of concern for future improvements. These baselines and graphs can be used annually to compare progress and to track the areas which are becoming more mature and/or utilised. As stated previously, the organisation must determine operational targets for themselves which can be used for targets of improvement. Upon completion of the survey, follow-up cyberresilience assessment interviews were conducted at level 1 (security controls) as recommended by Malatji et al. (2021).

4.2.2 Interview findings

The interview protocol contained only four questions. The first two questions sought to determine the types of cybersecurity controls used in both the IT and ICS environments, and the perceived effectiveness and comprehensiveness scores for those controls. The effectiveness and comprehensiveness indexes needed to be computed in the subsequent data analysis using equations (1) and (2). From these two questions the cybersecurity controls were *classified* into either the social, technical and environmental dimensions as described by Malatji et al. (2020).

Subsequently, the JO index to determine the socio-technical cybersecurity vulnerability gaps to *optimise* the controls was computed. The *mature* process activity of the STS cybersecurity optimisation process (Malatji et al., 2020) was not necessary as it is inherently contained within the overall resilience assessment exercise in the STS CAM. The first two questions are the only required interview questions for the operationalisation of the STS CAM to evaluate the effectiveness and comprehensiveness of organisational security controls.

The last two questions sought to establish the existence and configuration of the cybersecurity governance structure, if any, and the types of cybersecurity incidents experienced. These questions are not essential for the operationalisation of the STS CAM. They emanated from the pre-survey workshops as follow-up questions for the interviews. This therefore implies that each case study pre-survey workshop may prompt different follow-up interview questions. Moreover, there was a sentiment in the pre-survey workshop that matters pertaining to cybersecurity are the purview of IT, and not ICS. This prompted the researchers to phrase the ensuing interview questions differently from those of IT for the ICS participant.

Ultimately, though, the ICS cybersecurity interview questions, although phrased differently, still elicited the same data as that from IT: a list and appraisal of security controls in terms of the effectiveness and comprehensiveness indexes. Unlike the survey questionnaire where the discrete value scale had fixed options to select from, interviewees could score the

effectiveness and comprehensiveness of each cybersecurity control with any value from 0-100% (i.e. 0,000-1,000). The IT security controls interview results are presented in Table 3.

Table 3. Case 1 interview results

IT security controls (Level 1 cybersecurity practices)	Effectiveness score	Comprehensiveness score
Firewall	0,750	0,850
Anti-malware	0,800	0,850
Group/security policy	0,650	0,650
Security bulletin (awareness & training)	0,500	0,500
Physical security	0,700	0,600
Desktop research and industry reports reading	0,500	0,500
Regulatory compliance and statutory requirements	0,500	0,500
IT team for security issues	0,500	0,500

To classify the IT security controls into either the social, technical or environmental dimensions, the STS dimension attributes detailed by Malatji et al. (2020) were utilised. These essentially have five main domains – (i) organisational structure (business functions) and (ii) actors (people) under the social dimension; (iii) technology (technical tools and resources) and (iv) work activities (tasks) under the technical dimension; and (v) environment under the environmental dimension. This is the STS classification tool applied to the IT security controls in Table 3. The STS classification results are shown in Table 4.

Table 4. STS classification of IT security controls

STS dimension	STS domain	Categorised IT security controls
Social	Organisational structure *(Functions)*	Human-driven physical security Security bulletin (awareness & training) Group policy (speaks to governance) Desktop research and industry reports reading (knowledge)
	Actors *(People)*	IT team
Technical	Technology *(Technical tools & resources)*	Firewall Anti-malware Security policy Systems-driven physical security
	Work activities *(Tasks)*	*None specifically defined*
Environmental		Regulatory compliance and statutory requirements

Although there were only eight IT security controls in Table 3, two security controls gave rise to an additional two according to the STS dimension attributes criteria as shown in Table 4. These are physical security, divided into the *systems-driven physical security* (e.g. video surveillance and biometric access control were mentioned) and *human-driven physical security* (e.g. security guards) and the group/security policy, subdivided into *security policy* and *group policy*, which speaks more to governance. The interviewee indicated that they use the COBIT framework only for IT governance as a regulatory compliance and statutory requirement. They do not use the COBIT 5 for Information Security aspect of the framework

at all. Furthermore, the IT operations have no formalised cybersecurity governance structure. IT security issues are distributed among the IT team members on an ad hoc basis. The types of incidents they have experienced include:

- Email spoofing
- Laptops stolen from premises
- Denial-of-service attack via ping floods
- Email spam
- Internet protocol blacklisting

By applying equation (1), the overall *effectiveness index = 0,598* and *comprehensiveness index = 0,596*. These were computed based only on the available security controls and can be misleading. This is where the STS approach comes in. Based on the STS classification in Table 4 and using only the individual effectiveness scores in Table 3, applying equation (1) shows that the overall *social* X_b *= 0,570, technical* Y_b *= 0,725* and *environmental* Z_b *= 0,500*. To compute the JO_{before}, equation (2) was applied. The JO state before security intervention efforts are applied in security areas of concern is JO_{before} = 0,117. According to Malatji et al. (2020), this is the baseline measurement where follow-up measurements (JO_{after}) after a year or so are expected.

The following JO interpretations should be applied (Malatji et al., 2020): (i) $JO_{before} < JO_{after}$ means security has deteriorated; (ii) $JO_{before} = JO_{after}$ means security has neither improved nor deteriorated; and (iii) $JO_{before} > JO_{after}$ means security has improved. The JO index is used only for this purpose and has no other quantitative meaning. Moreover, the concept of JO does not mean that the three STS dimensions must all be equal. It only means that all effectiveness scores in the dimensions should add up to 100% for socio-technical cybersecurity vulnerability gaps to not exist. The WSP's data indicates that the security measures are more emphasised towards the higher score of the three STS dimensions, in this case technical Y_b = 0,725, and less emphasised on the lower score, environmental Z_b = 0,500. It should, however, be noted that the determination of which is the highest and lowest score depends on the target or baseline score against which the comparison is made. For example, if the baseline score is 0,500, then there is no lower score as all three STS dimensions scored 0,500 and above.

If we assume that the environmental dimension Z_b = 0,500 has the lowest score, then a drilldown exercise for future security intervention efforts would have to be conducted on the environmental dimension. The individual security controls with lower effectiveness scores are where intervention efforts for improvement should be introduced. The CI cybersecurity capability framework lists a few cybersecurity *control* standards, guidelines and frameworks,

as recommended by NIST (2018), and these can be adopted for implementation of the CI cybersecurity capability framework to improve cybersecurity areas of concern. One of the recommended frameworks is the COBIT 5 for Information Security. This framework's security controls have been STS-classified in detail by Malatji et al. (2020). If Table 4 were compared to the STS-classified COBIT 5 for Information Security controls, it would be apparent that the WSP's enterprise IT security controls are not only inadequate, but that both the effectiveness and comprehensiveness scores would probably be much lower. In the ICS environment, cybersecurity controls extracted from the interview transcript are presented in Table 5.

Table 5. Interview: ICS cyberresilience assessment results

ICS security controls (Level 1 security practices)	**Effectiveness score**	**Comprehensiveness score**
Granting of permits to work on plant and specific sections for repair and maintenance *(human-driven physical security)*	0,500	0,500

The emphasis throughout the interview was that the WSP's processes for water quality and access to plants are very manual. There are no automated early warning systems to monitor, for example, water pressure, flows or quality changes. Considering that a control room operator typically makes supervisory decisions via the human-machine interface (HMI) to monitor and control industrial processes (NIST, 2015; Panguluri, William, & Clark, 2004), the WSP is likely operating second-, if not, first-generation supervisory control and data acquisition (SCADA) systems (Alexandru, 2016; Stellios, Kotzanikolaou, & Psarakis, 2019).

It would, however, be premature to conclude that the industrial automation and process control systems of the WSP are air-gapped – a term referring to ICS networks that are not connected to the Internet, enterprise IT network and/or any unsecured networks. A physical inspection of the facilities and the monitoring and evaluation of the control and field networks, including network access points of the WSP's OT systems, would be required before reaching any conclusions. However, the interview data indicates that this is a likely scenario. The data further indicates that the only connection the WSP's ICS operators currently have with the IT network is through access to emails and other enterprise tools such as spreadsheets, word processors and the Internet.

This explains why the ICS interviewee thought that all computer systems security-related matters fall under the purview of the IT team. This is precisely the type of attack surface an experienced cyberattacker needs to establish a foothold – reconnaissance – through the enterprise IT network and move laterally to the ICS network. After all, a communication link between the enterprise/information systems environment (level 4 ICS architecture) or enterprise IT network and SCADA/HMI environment (level 3 ICS architecture) or ICS network

is attained through open communication protocols such as the Internet (Hahn, 2016; Krotofil, Kursawe, & Gollmann, 2019; Sullivan, Luiijf, & Colbert, 2016).

Air-gapping and/or network isolation is therefore recommended as one of the better security options in ICS environments. It provides a fail-safe mechanism against propagated malware (Dickson & Goodwin, 2020). A formal governance structure exists in the WSP to monitor the quality of water through a risk-based incident management protocol – water safety plan. As mentioned earlier, this protocol is very manual and lacks a digital early warning system mechanism as acknowledged by the ICS interviewee. Moreover, none of these protocols speak to cyberresilience of the water CI. The WSP has so far not reported any major physical or cyberincident that they are aware of on their water CI.

To quantify the ICS cyberresilience vulnerability gaps through the STS approach, the human-driven physical security control in Table 5 is classified in the social dimension. Similarly, if security controls in Table 5 were compared to controls, whether STS-classified or not, in standards, guidelines and frameworks such as the ISA/IEC 62443 and NIST Special Publication 800-53 as recommended by NIST (2018), it would be apparent that the WSP's ICS environment has no cyberresilience controls. These standards, guidelines and frameworks provide a catalogue of security and privacy controls for organisations and CI owners/operators to protect their assets. To protect assets from a wide array of threats such as malicious cyberattacks, adverse weather and natural events, (un)intentional human errors and aging infrastructure, the WSP needs to benchmark against best practices. This is where the CI cybersecurity capability framework comes in.

4.2.3 Conclusion

The WSP has no structured method to address enterprise IT security incidents, be it through a standard, guideline or framework. The IT unit uses the COBIT framework but only for governance as a regulatory compliance and statutory requirement. The information security aspect of the COBIT framework is not being utilised in any way. The survey data indicates a relatively good utilisation of the approach to identifying, authenticating and authorising employees, vendors and other partners to access IT systems at the WSP. Utilisation of the IT security response improvement plan is also perceived to be relatively good. However, the maturity of these approaches is very poor, as indicated in Figure 8. This aligns with the fact that the WSP has no structured framework approach to address enterprise IT security incidents.

Furthermore, the ad hoc security controls that the WSP has emphasise more the technical dimension than the social (which includes human behaviour and (un)intentional human errors) and environmental dimensions. This opens socio-technical cybersecurity vulnerability gaps in the less emphasised security dimensions. A good example is that laptops were stolen right out of the WSP's office premises. In addition, an irate employee on suspension ping-flooded the WSP's public IP address, resulting in a temporary denial of services. These two examples demonstrate the human-made breaches (social dimension). This means that even if security practices are present and mature, if they are not being utilised, then breaches will always occur. For example, the IT system access privileges of the employee on suspension should have been (temporarily) limited or revoked by one of the IT team members (human, then technical).

On the ICS side, it is safe to conclude that apart from the human-driven physical security measure of controlling access to sections of a plant by paper-based permits for mostly repair and maintenance, no formalised ICS cybersecurity practices exist. This is in line with the ICS participant's perception that all computer systems security-related matters are handled by enterprise IT. The WSP's water and wastewater CI is therefore neither secure against nor resilient to malicious cyberattacks, adverse weather and natural events, (un)intentional human errors and aging infrastructure. The WSP needs a formalised security operations centre (SOC) to accommodate both the enterprise IT and ICS cybersecurity requirements. Dedicated teams should be established to cater for each area's specialised security practices. Bearing in mind that many cyber events go undetected (Lees et al., 2018), the overall findings of the study are that the WSP is not cyberresilient in either the enterprise IT or ICS environments. An advanced persistent threat actor or nation state could easily compromise the WSP's cyber defences if there is sufficient motivation.

4.3 Case study 2

The second case study was a water establishment headquartered in the KwaZulu-Natal Province of South Africa. Two participants, both from enterprise IT, took part in the study. Although no specific participant from the ICS environment took part in the study, the IT participants did indicate that some aspects of ICS/SCADA security activities are handled by enterprise IT. Together, the two IT participants were at tactical and operational levels.

4.3.1 Survey findings

On the survey closing date both IT participants had completed the survey. The water cyberresilience assessment results from the survey are shown in Table 6 below. Like the first case study, the assessment was conducted at level 2 cybersecurity practices (140

cybersecurity capabilities), and the results in Table 6 have thus been rolled up to level 3 cybersecurity practices (29 cybersecurity capability domains). The results are based on the discrete value scale described in Figure 8.

Table 6. Case 2 survey results

Level 3 (Cybersecurity capability domain)	**Maturity**	**Utilisation**
Asset management	0,729	0,708
Business environment	0,675	0,725
Governance	0,563	*0,438*
Risk assessment	0,688	0,563
Risk management strategy	0,750	0,750
Supply chain risk management	0,575	0,550
Cloud security asset management	0,625	*0,125*
Cloud security off-site activities	0,696	0,696
Identity management, authentication and access control	*0,250*	*0,250*
Data security	0,625	0,609
Mobile computing devices security	*0,294*	*0,288*
Information protection processes and procedures	0,740	0,688
Cryptography	*0,000*	*0,000*
Maintenance	0,813	0,875
Protective technology	0,625	0,600
Audit assurance	0,875	0,500
Awareness and training	0,750	0,725
Anomalies and events	0,625	0,600
Cybersecurity research and development	0,625	*0,125*
Security continuous monitoring	0,813	0,781
Detection processes	0,725	0,600
Response planning	*0,250*	*0,250*
Response communications	0,725	0,525
Analysis	0,575	0,450
Mitigation	0,625	0,583
Response improvements	*0,438*	*0,250*
Recovery planning	0,625	0,500
Recovery improvements	0,750	0,750
Recovery communications	0,708	0,500
Overall	**0,612**	**0,517**

The same 29 cybersecurity capability domain results are presented as a spider graph in Figure 12.

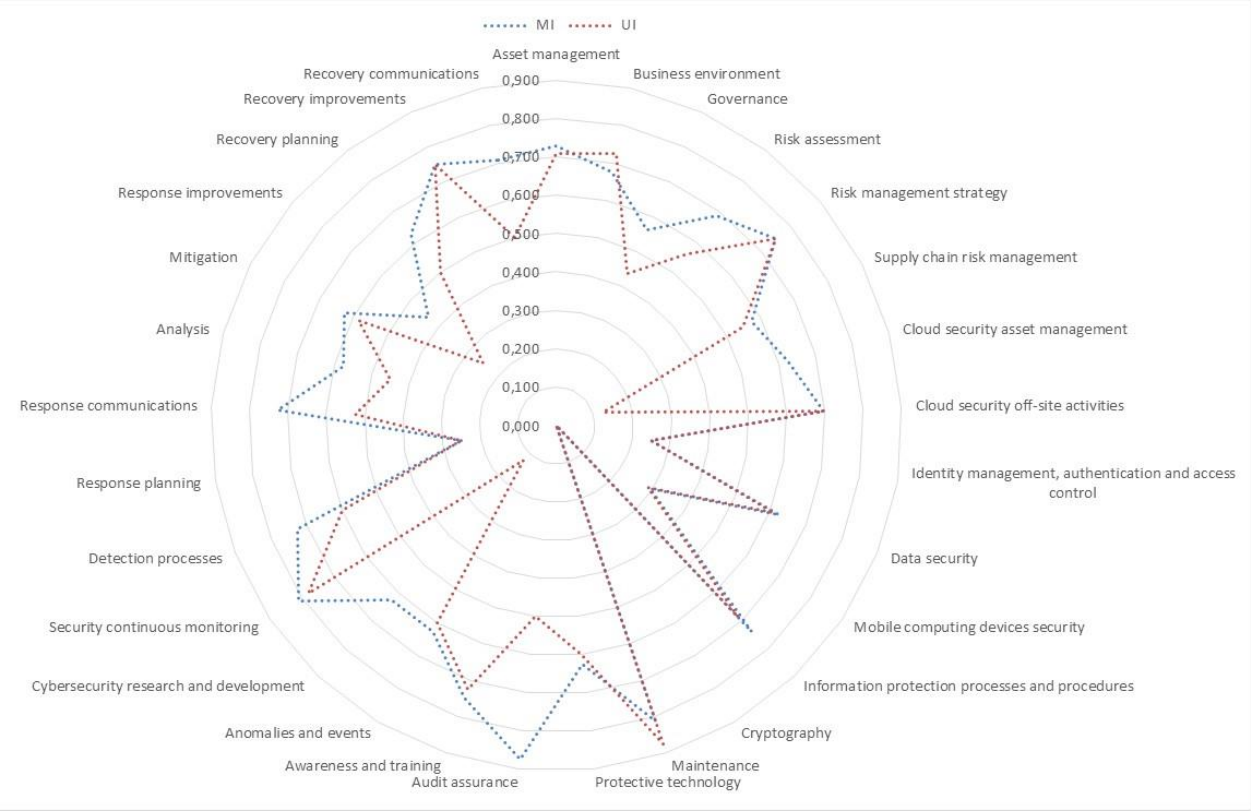

Figure 12. Spider graph visualisation of case 2 survey results

It can be seen from Table 6 and Figure 12 that 24 out of 29 cybersecurity capability domains received a maturity index score above 0,500 (good). Moreover, three cybersecurity capability domains were maturity scored above 0,750 (very good). These are:

- Maintenance
- Audit assurance
- Security continuous monitoring

This means that a good measure of the 140 cybersecurity capabilities received a maturity index score above 0,500 (good) in the survey. There are only five security areas of concern in terms of maturity as italicised in Table 6. The maturity baseline of this water entity can be visualised as shown in Figure 13.

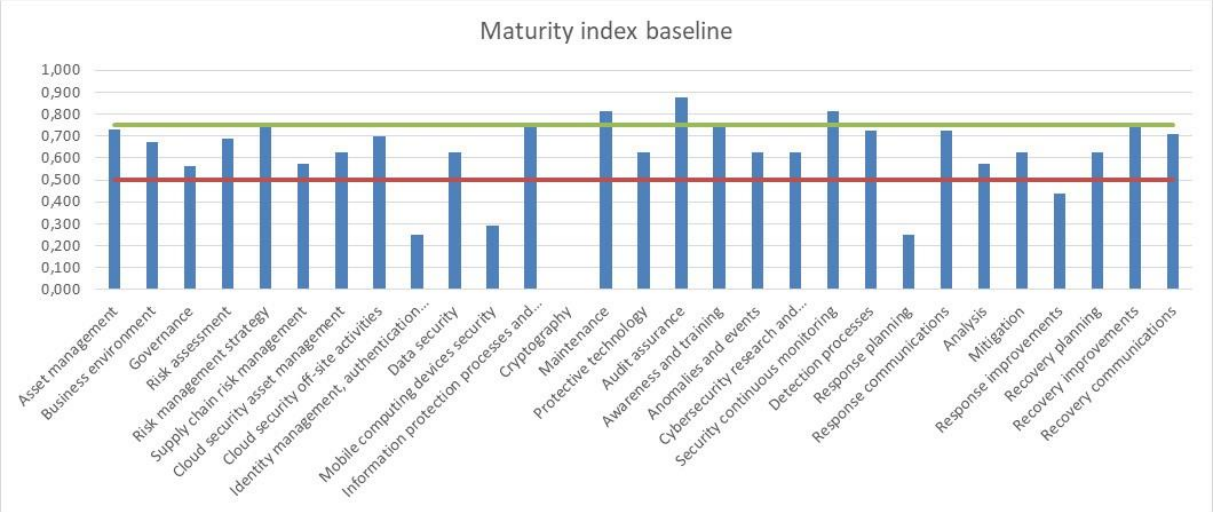

Figure 13. Case 2 maturity index graph

It can be seen from Figure 13 that most of the cybersecurity capability domains rank above the 0,500 mark, with three above 0,750 and many just below 0,750. With reference to Table 6, 21 out of 29 cybersecurity capability domains received a utilisation index score above 0,500 (good). Similarly, this means that a good measure of the 140 cybersecurity capabilities received a utilisation index score above 0,5 (good) in the survey. The entity scored above 0,500 (good) in the utilisation index of 20 cybersecurity capability domains where two scored above 0,750 (very good). These are:

- Maintenance
- Security continuous monitoring

There are eight security areas of concern in terms of utilisation as italicised in Table 6. The utilisation baseline of this water entity can be visualised as shown in Figure 14.

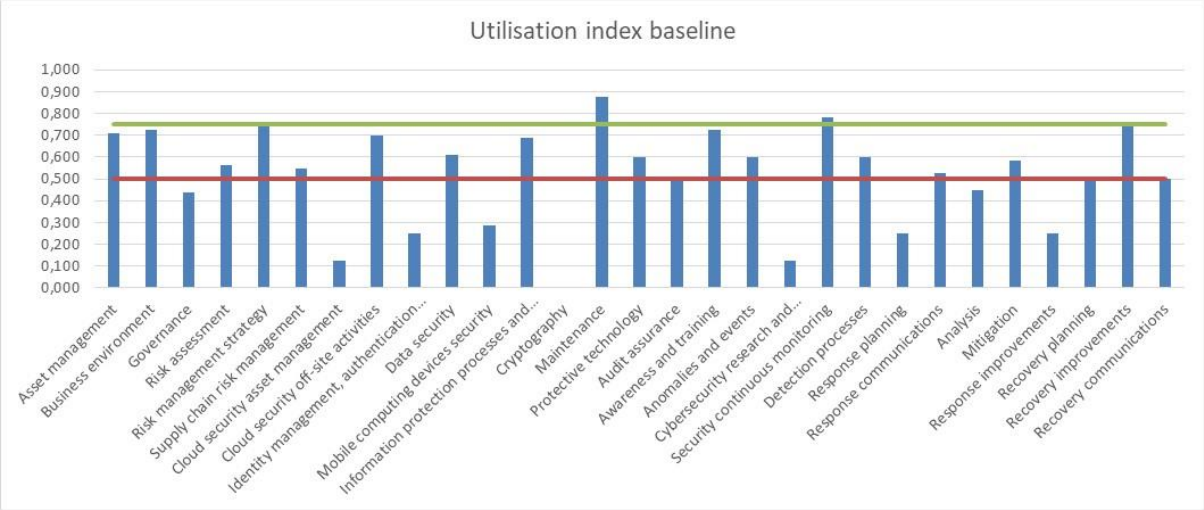

Figure 14. Case 2 utilisation index graph

Most of the cybersecurity capability domains rank above the 0,500 mark of utilisation, with two above 0,750 and many just below 0,750. Figures 11 and 12 indicate to the water entity which areas of cybersecurity can be improved upon and which are functioning at the international best practice of 0,750. As this is self-reported, the survey results in Table 6 mean that the participants believed the water entity's maturity and utilisation of cybersecurity resilience practices were generally good to very good. Upon completion of the survey, follow-up cyberresilience assessment interviews were conducted at level 1 (security controls) as recommended by Malatji et al. (2021).

4.3.2 Interview findings

The interview results pertaining to the first two questions which sought to determine the types of cybersecurity controls applied in both the IT and ICS environments, and the perceived effectiveness and comprehensiveness scores for those controls, are shown in Table 7.

Table 7. Case 2 interview results

IT security controls (Level 1 cybersecurity practices)	**Effectiveness score**	**Comprehensiveness score**
Firewall	0,800	0,800
Governance policies	0,400	0,500
Encryption	0,000	0,000
Anti-malware	0,700	0,800
User awareness & training	0,500	0,600
Systems-driven physical security (biometrics by authorisation level)	0,900	0,900
Technical security policies	0,400	0,500
Processes	*Not allocated*	*Not allocated*
Cybersecurity strategy	*Not allocated*	*Not allocated*
User access control to systems	*Not allocated*	*Not allocated*
Email security tools	*Not allocated*	*Not allocated*
Intrusion detection and prevention systems	*Not allocated*	*Not allocated*
Cybersecurity framework	*Not allocated*	*Not allocated*
Human-driven physical security	*Not allocated*	*Not allocated*
Web security tools	*Not allocated*	*Not allocated*
AI-based network monitoring tool	*Not allocated*	*Not allocated*

It can be seen from Table 7 that the italicised security controls were not allocated effectiveness and comprehensiveness scores. These fell through the cracks somewhere during the one-to-one virtual conversation. This brings the efficacy of the interview method into question for eliciting this type of information. Nonetheless, the overall effectiveness of the organisation's cybersecurity controls can be estimated to be 6 out of 10, and comprehensiveness is estimated to be 5 out of 10, at least according to the interviewee. This means that the

cybersecurity controls with no score allocation in Table 7 will at minimum have an effectiveness score of 6 out of 10 and a comprehensiveness score of 5 out of 10. The STS classification results are shown in Table 8.

Table 8. STS classification of IT security controls

STS dimension	STS domain	Categorised IT security controls
Social	Organisational structure *(Functions)*	Human-driven physical security User awareness & training Governance policies
	Actors *(People)*	IT team Remote workers Users
Technical	Technology *(Technical tools & resources)*	AI-based network monitoring tool Anti-malware Cybersecurity framework Cybersecurity strategy Encryption Email security tools Firewall Intrusion detection and prevention systems Processes Security policy Systems-driven physical security User access control to systems Web security tools
	Work activities *(Tasks)*	Awareness through employee onboarding process
Environmental		Datacentre

Based on the STS classification in Table 8 and using effectiveness scores of only those controls which were allocated scores in Table 7, STS computations were made. Applying equation (1) shows that the overall *social* $X_b = 0{,}450$, *technical* $Y_b = 0{,}600$ and *environmental* $Z_b = 0{,}600$. The datacentre score was allocated based on the overall effectiveness score of the entire organisation as estimated by the interviewee. As in the first case study, if the baseline score for comparison is set at 0,500, then the social dimension has the lowest score of the three dimensions as it is lower than 0,500. This is where further investigation of the controls in the social dimension is required to ensure that no socio-technical vulnerability gaps exist. To compute the JO_{before}, equation (2) was applied. The JO state before security intervention efforts are applied in security areas of concern is $JO_{before} = 0{,}231$.

In the ICS environment, no study participant was available. However, the IT interviewee indicated that enterprise IT has implemented firewalls between their network and the ICS network to ensure that governance takes place as far as organisational user access control is concerned, even with SCADA systems. There are no dedicated ICS cybersecurity specialists within the organisation's SOC. Only enterprise IT currently handles network and user access control related cybersecurity matters on behalf of the ICS operators.

The third interview question sought to establish the existence and configuration of the cybersecurity governance structure. It was found that the organisation has a fully-fledged SOC

to provide the incidents management function. However, it was highlighted by the interviewee that the cybersecurity function at the organisation, including within the SOC, does not have sufficient cybersecurity specialists. The final interview question sought to establish the types of cybersecurity incidents experienced so far. The only major cybersecurity incident is whale phishing.

4.3.3 Conclusion

The water entity has a structured approach to addressing enterprise IT security incidents through a cybersecurity framework and strategy. In addition, the entity has an AI-based tool to monitor network traffic as well as a SOC to manage cybersecurity incidents. Because a few cybersecurity controls did not have scores allocated, the STS scores were computed with incomplete data and are therefore not reliable. The interview method for eliciting cybersecurity controls data should therefore be revised for more complete, reliable and valid data.

On the ICS side, the network traffic is monitored through an AI-based tool operated by the enterprise IT. Moreover, the enterprise IT handles the user access groups and authorisation profiles for the ICS environment. Although there are no dedicated ICS cybersecurity specialists at the entity, the overall findings of the study are that the entity is relatively cyberresilient in both the enterprise IT and ICS environments.

4.4 Case study 3

The third case study was a water entity headquartered in the North-West Province of South Africa. Two participants, both from enterprise IT, took part in the study. As in case study 2, no specific participant from the ICS environment took part in the study. However, the IT participants did indicate that some aspects of ICS/SCADA security have been transferred to enterprise IT. Together, the two enterprise IT participants were at tactical and operational levels.

4.4.1 Survey findings

On the survey closing date both IT participants had completed the survey. The water cyberresilience assessment results from the survey are shown in Table 9 below. As in the previous case studies, the assessment was conducted at level 2 cybersecurity practices (140 cybersecurity capabilities), and the results in Table 9 have, similarly, been rolled up to level 3 cybersecurity practices (29 cybersecurity capability domains). The results are based on the discrete value scale described in Figure 8.

Table 9. Case 3 survey results

Level 3 (Cybersecurity capability domain)	Maturity	Utilisation
Asset management	0,729	0,646
Business environment	0,775	0,550
Governance	*0,375*	*0,438*
Risk assessment	0,500	*0,313*
Risk management strategy	0,833	0,708
Supply chain risk management	*0,325*	*0,200*
Cloud security asset management	*0,188*	*0,125*
Cloud security off-site activities	0,679	0,625
Identity management, authentication and access control	*0,333*	*0,250*
Data security	0,766	0,703
Mobile computing devices security	*0,219*	*0,181*
Information protection processes and procedures	0,729	0,698
Cryptography	*0,208*	*0,167*
Maintenance	0,688	0,563
Protective technology	0,825	0,800
Audit assurance	0,708	0,708
Awareness and training	0,800	0,750
Anomalies and events	0,675	0,575
Cybersecurity research and development	*0,250*	*0,375*
Security continuous monitoring	*0,375*	*0,484*
Detection processes	*0,475*	*0,350*
Response planning	*0,125*	*0,125*
Response communications	*0,400*	*0,350*
Analysis	*0,400*	*0,375*
Mitigation	*0,292*	*0,333*
Response improvements	*0,000*	*0,000*
Recovery planning	*0,375*	*0,250*
Recovery improvements	*0,000*	*0,000*
Recovery communications	*0,333*	*0,375*
Overall	**0,461**	**0,414**

The same 29 cybersecurity capability domain results are presented as a spider graph in Figure 15.

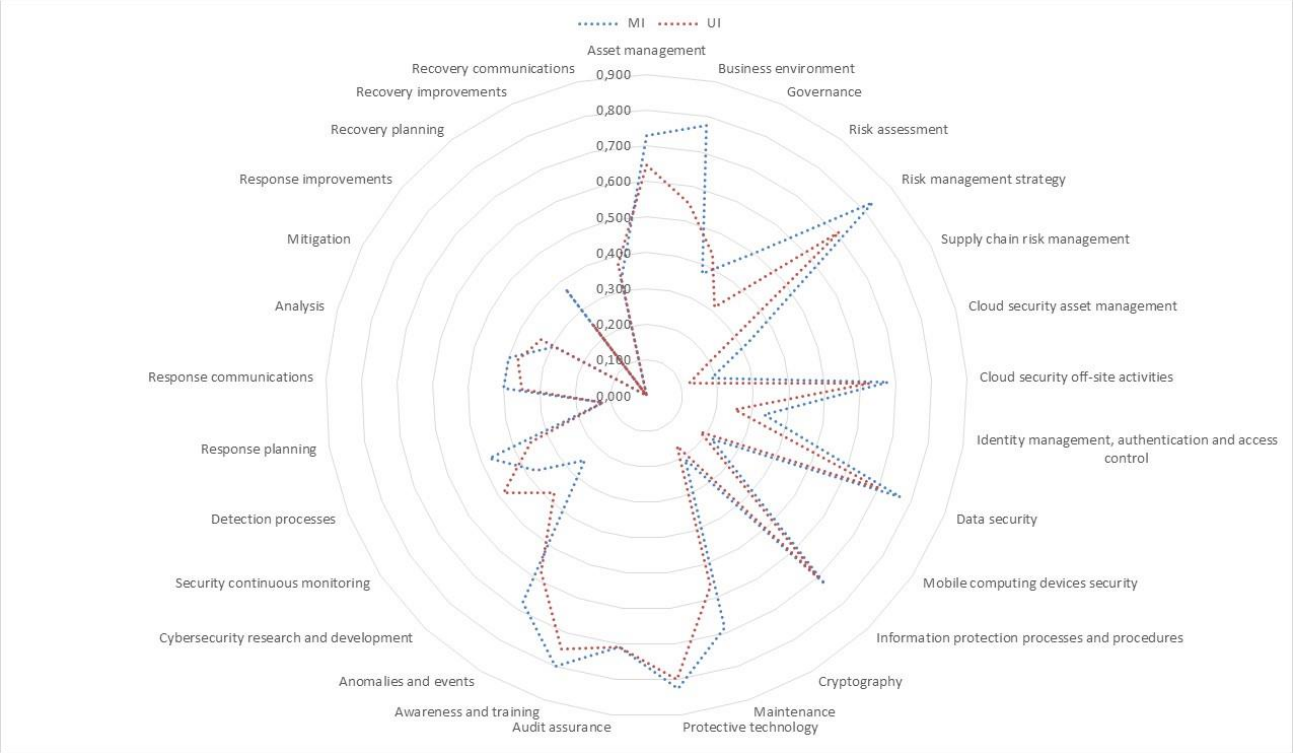

Figure 15. Spider graph visualisation of case 3 survey results

It can be seen from Table 9 and Figure 15 that only 12 out of 29 cybersecurity capability domains received a maturity index score above 0,500 (good). Moreover, 5 cybersecurity capability domains received maturity scores above 0,750 (very good). These are:

- Business environment
- Risk management strategy
- Data security
- Protective technology
- Awareness and training

This means that a good measure of the 140 cybersecurity capabilities received a maturity index score below 0,500 (good) in the survey. This translates to 17 security areas of concern in terms of maturity, as italicised in Table 9. The maturity baseline of this water entity can be visualised as shown in Figure 16.

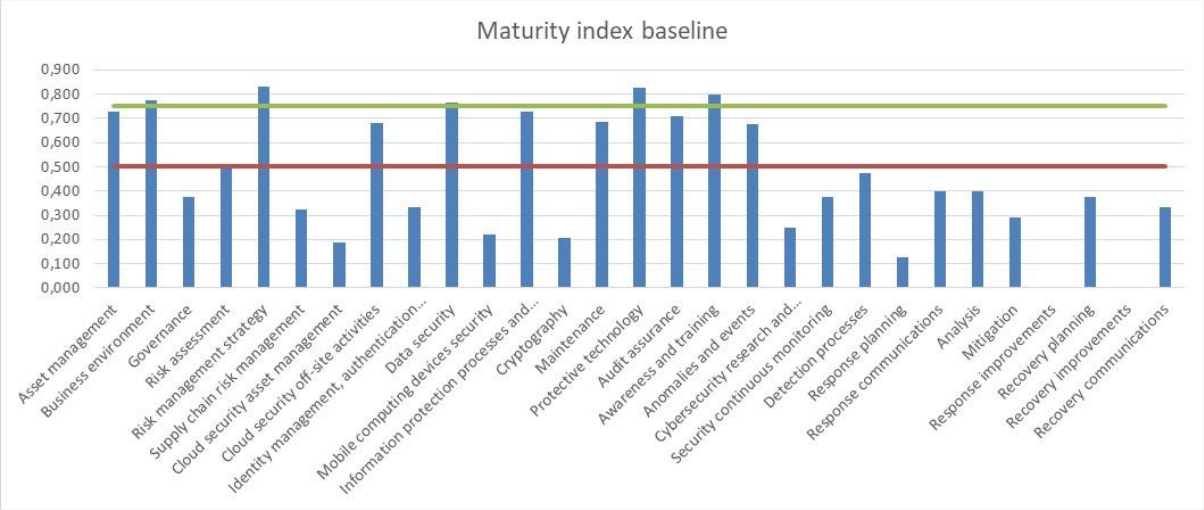

Figure 16. Case 3 maturity index graph

It can be seen from Figure 16 that most of the cybersecurity capability domains rank below the 0,500 mark, with only five above 0,750 and three just below 0,750. 11 out of 29 cybersecurity capability domains received a utilisation index score above 0,500 (good) with only one – protective technology – scoring above 0,750 (very good). This means that a good measure of the 140 cybersecurity capabilities received a utilisation index score below 0,500 (good) in the survey. This translates to the entity scoring below 0,500 (good) on 18 cybersecurity capability domains, meaning that the water entity has 18 security areas of concern in terms of the utilisation of its cybersecurity practices, as italicised in Table 9. The utilisation baseline of this water entity can be visualised as shown in Figure 17.

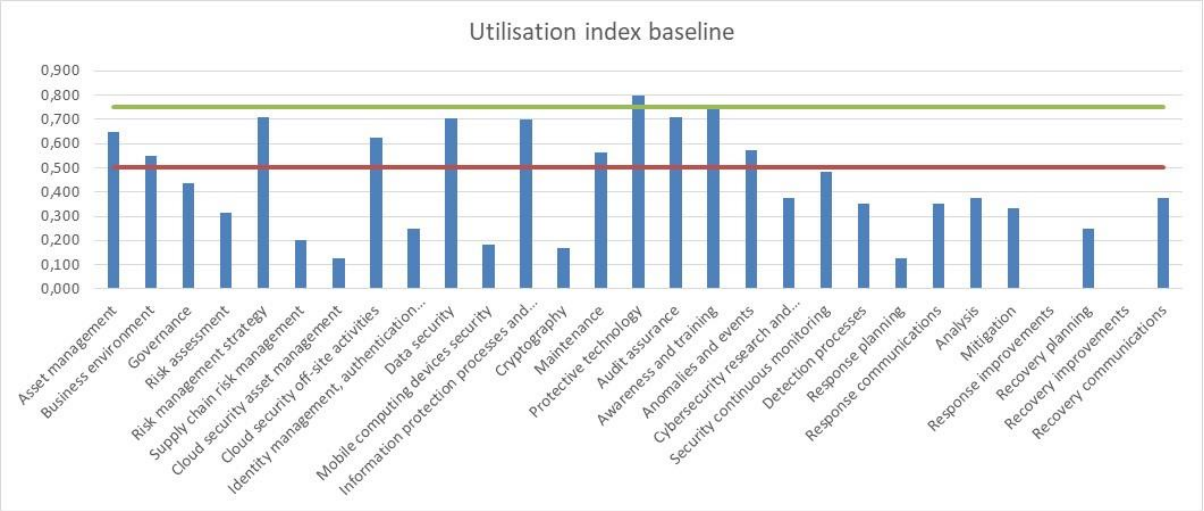

Figure 17. Case 3 utilisation index graph

Most of the cybersecurity capability domains rank below the 0,5 mark of utilisation, with one above 0,750 and three just below 0,750. Figures 17 and 18 indicate to the water entity which areas of cybersecurity can be improved upon and which are functioning at the international

best practice of 0,750. It is clear from these self-reported survey results that the participants believed that the water entity's maturity and utilisation of cybersecurity resilience practices are below par. The entity should address the identified areas of security concern. In particular, the entity scored very low in the response and recovery aspects of their cybersecurity practices. This means that they are likely to take a significant amount of time to respond to and recover from adverse conditions, stresses, attacks and/or compromises. In fact, the overall maturity and utilisation index scores are both below the 0,500 (good) baseline, as indicated in Table 9. Follow-up cyberresilience assessment interviews were conducted and the results are as follows.

4.4.2 Interview findings

Two participants were interviewed separately at this water entity. Quantitative scores to similar objects of measure were averaged into a single score and the rest are given as separate scores. Four main questions were asked, and the first question sought to determine the types of cybersecurity controls in place in both the enterprise IT and ICS environments. The second question sought to establish the perceived effectiveness and comprehensiveness scores for these controls. Interview results are shown in Table 10.

Table 10. Case 3 interview results

IT security controls (Level 1 cybersecurity practices)	**Effectiveness (Actual usage by employees)**	**Comprehensiveness (IT security safeguards)**
Antivirus software	0,600	0,950
Cybersecurity policy and procedures	0,850	0,850
Daily backups	0,950	0,950
Disaster recovery plan	0,950	0,850
Encryption	0,950	0,950
Firewall	0,950	0,950
IT steering committee	0,500	0,500
Laboratory information management system (LIMS) application security	0,500	*0,250*
Mobile devices security	*0,475*	*0,475*
Patch management	0,700	0,700
Physical security/access control	*0,475*	*0,325*
Security governance framework	0,950	0,950
Systems access control (includes password policy)	0,725	0,850
User awareness and training	0,850	0,850
Vulnerability scans	*0,400*	0,600
SCADA access control security	0,725	0,475
Cloud security policy	*0,000*	*0,000*
Remote working security policy	*0,000*	*0,000*
Holistic database security policy	*0.00*	*0.00*

It can be seen from Table 10 that three security controls were allocated effectiveness and comprehensiveness scores of 0. These are currently being implemented in the organisation. In other words, these are required controls but currently absent, which is the definition of a 0,000 score in the discrete value scale utilised in the study. Regarding the implemented security controls, there are three areas of concern in both the effectiveness (actual usage by employees) and comprehensiveness (implemented IT security safeguards) of the security controls, as italicised in Table 10. The effectiveness security areas of concern are:

- Physical security/access control
- Mobile devices security
- Vulnerability scans

The comprehensiveness security areas of concern are:

- Physical security/access control
- Mobile devices security
- LIMS application security

The identified areas of concern at level 1 cybersecurity practices (security controls) are consistent with the findings at level 2/3 cybersecurity practices (cybersecurity capabilities and domains) from the previous section. This is because, for example, the physical security/access control belongs to the identity management, authentication and access control domain; mobile devices security to the mobile computing devices security domain; and vulnerability scans to the detection processes domain, as referenced from Table 9. The STS classification of the interview results are shown in Table 11. The actors and environmental factors were derived from the interview transcript as some do not appear in Table 10.

Table 11. STS classification of IT security controls

STS dimension	STS domain	Categorised IT security controls
Social	Organisational structure *(Functions)*	Human-driven physical security Security governance framework User awareness & training
	Actors *(People)*	IT steering committee IT team Remote workers Users
Technical	Technology *(Technical tools & resources)*	Anti-virus software Cloud security policy Cybersecurity policy and procedures Daily backups Disaster recovery plan and procedure Encryption Firewall Holistic database security policy LIMS application security Mobile devices security Patch management Remote working security policy Systems access control (includes password policy)
	Work activities *(Tasks)*	Vulnerability scans
Environmental		Service provider Government

Based on the STS classification in Table 11 and using effectiveness scores in Table 10, STS computations were made. Applying equation (1) and using effectiveness scores of *only* the scored security controls in Table 11 shows that the *overall social* $X_b = 0{,}694$, *technical* $Y_b = 0{,}581$ and *environmental* Z_b = *indeterminate*. The environmental dimension is indeterminate because the service provider and government as identified from the interview were not allocated a score. Once again, the efficacy of the data collection methods utilised, and not the data analysis techniques, needs strengthening. As the *environmental dimension* (Z_b) is indeterminate, JO cannot be computed using equation (2). Furthermore, the technical dimension ($Y_b = 0{,}581$) has a lower score than the social dimension. Further investigations of the water entity's security controls are therefore required in the technical dimension to ensure closure of any security vulnerability gaps. This is in alignment with the italicised interview results in Table 10.

Regarding the ICS environment, it was indicated that the water entity has just taken over the entire operation of the SCADA systems from a service provider that had managed this on their behalf for many years. This arrangement was, and to a certain extent still is, a security risk. As shown in Table 10, the only ICS security control the water entity is managing, through the enterprise IT department, is the SCADA access control security. In other words, there are no dedicated ICS cybersecurity specialists within this water entity either. Moreover, other applicable ICS security controls, some of which are contained within the capability domains in Table 9, are not currently being addressed by the water entity. This poses a serious risk to the entity's drinking water supply systems that are either exposed to the entity's enterprise

computer network or accessible remotely by third parties such as the previous service provider.

The third interview question sought to establish the existence and configuration of the cybersecurity governance structure. It was found that the water entity has no formal SOC for the incidents management function. This is not necessarily a bad thing, as SOCs are recommended for larger organisations. For relatively smaller to medium-sized organisations such as this water entity, a structured approach by enterprise IT through a governance framework is adequate. In this regard, it was highlighted by the interviewee that the organisation does follow COBIT for both its IT and information security governance. However, it was revealed that the organisation addresses security breaches reactively or as and when they occur. In addition, any member of the IT team can be allocated the task of investigating a solution regardless of their security skill set and/or experience. This points to either a shortage of security personnel, non-adherence to the COBIT for Information Security framework, or both. The non-adherence to the COBIT framework could impact on both cybersecurity performance and compliance requirements.

The final interview question sought to establish the types of cybersecurity incidents experienced so far. The only major self-reported incident is a physical security breach where laptops, tablets and other portable items were stolen.

4.4.3 Conclusion

The water entity appears to have a structured approach, through COBIT, to address enterprise IT security incidents. In practice and as reflected in both the survey and interview results, the entity follows an ad hoc approach to manage cybersecurity controls. As corroborated in the interviews, the core issue is a shortage of cybersecurity skills and budget cuts. As in the previous case study, a few cybersecurity controls did not have scores allocated. Therefore, the STS scores were computed with incomplete data and are thus indicative and not entirely reliable. The interview method for eliciting cybersecurity controls data should therefore be revised for more complete, reliable and valid data. On the ICS side, the entity has numerous SCADA systems security controls either not implemented or still under the control and management of the previous service provider. The study concludes that the entity is not cyberresilient in either the enterprise IT or ICS environments.

4.5 Case study 4

The fourth case study was a water establishment headquartered in the Gauteng Province of South Africa. Two participants, both from the ICS environment, took part in the study. In this case organisation, no participants from the enterprise IT environment took part in the study. The ICS environment at this water establishment is completely air-gapped and has its own

domain separate from that of the enterprise IT. Together, the two ICS participants were at tactical and operational levels.

4.5.1 Survey findings

On the survey closing date both participants from the ICS environment had completed the survey. The water cyberresilience assessment results from the survey are shown in Table 12 below. As in the previous case studies, the assessment was conducted at level 2 cybersecurity practices (140 cybersecurity capabilities), and the results in Table 12 have, similarly, been rolled up to level 3 cybersecurity practices (29 cybersecurity capability domains). Moreover, the results are based on the discrete value scale previously described in Figure 8.

Table 12. Case 4 survey results

Level 3 (Cybersecurity capability domain)	**Maturity**	**Utilisation**
Asset management	0,646	*0,458*
Business environment	0,675	0,550
Governance	*0,219*	*0,156*
Risk assessment	*0,354*	*0,333*
Risk management strategy	*0,458*	*0,292*
Supply chain risk management	*0,375*	*0,325*
Cloud security asset management	*0,438*	0,500
Cloud security off-site activities	0,536	0,589
Identity management, authentication and access control	*0,458*	*0,333*
Data security	*0,469*	*0,438*
Mobile computing devices security	*0,338*	*0,256*
Information protection processes and procedures	0,594	*0,490*
Cryptography	0,583	*0,458*
Maintenance	0,688	0,625
Protective technology	0,525	0,525
Audit assurance	0,750	0,500
Awareness and training	0,725	0,650
Anomalies and events	0,575	0,550
Cybersecurity research and development	*0,375*	*0,125*
Security continuous monitoring	*0,344*	*0,313*
Detection processes	*0,425*	*0,375*
Response planning	0,500	0,500
Response communications	0,600	*0,375*
Analysis	*0,450*	*0,375*
Mitigation	0,542	*0,417*
Response improvements	0,500	*0,375*
Recovery planning	0,625	0,500
Recovery improvements	0,625	*0,375*
Recovery communications	0,542	0,542
Overall	**0,515**	**0,424**

The same 29 cybersecurity capability domain results are presented as a spider graph in Figure 18.

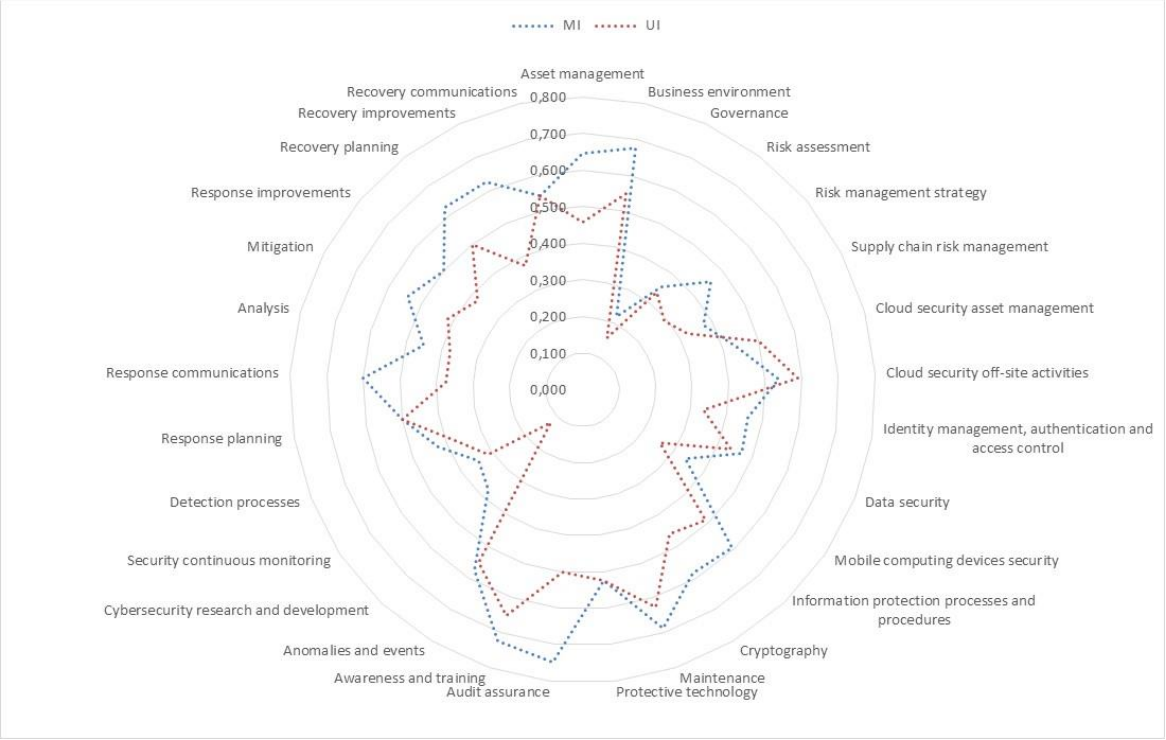

Figure 18. Spider graph visualisation of case 4 survey results

It can be seen from Table 12 and Figure 18 that 12 out of 29 cybersecurity capability domains received a maturity index score below 0,500 (good). Moreover, no single cybersecurity capability domain received a maturity score above 0,750 (very good). This means that a good measure of the 140 cybersecurity capabilities received a maturity index score below 0,500 (good) in the survey. This translates to 12 security areas of concern in terms of maturity, as italicised in Table 12. The maturity baseline of this water entity can be visualised as shown in Figure 19.

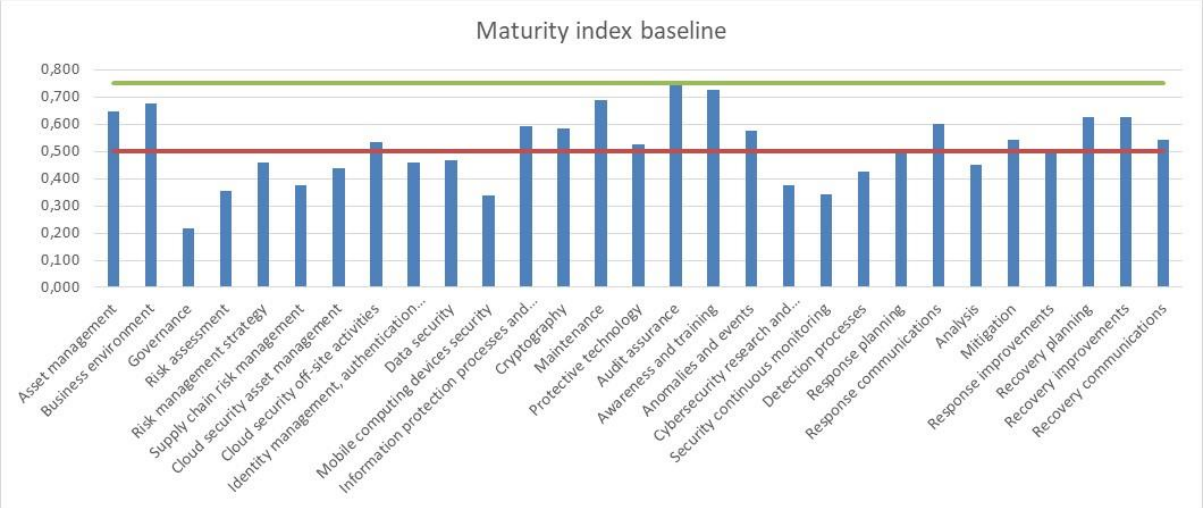

Figure19. Case 4 maturity index graph

It can be seen from Figure 19 that 15 cybersecurity capability domains rank above the 0,500 mark at this case study organisation, with two right on the 0,500 mark. Figure 19 also confirms that indeed no single cybersecurity capability domain received a maturity score above 0,750 (very good). 18 out of 29 cybersecurity capability domains received a utilisation index score below 0,500 (good), with no single score above 0,750 (very good). This means that a substantial number of the 140 cybersecurity capabilities received a utilisation index score below 0,500 (good) in the survey. It further means that the water entity has 18 security areas of concern in terms of the utilisation of its cybersecurity practices, as italicised in Table 12. The utilisation baseline of this water entity can be visualised as shown in Figure 20.

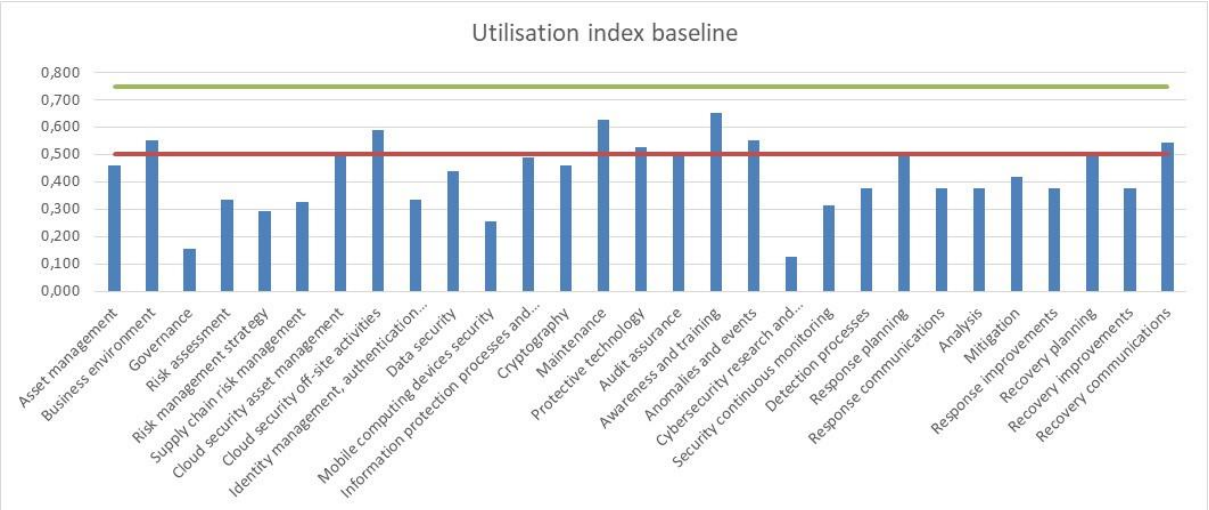

Figure 20. Case 4 utilisation index graph

Once again, Figure 20 confirms that most of the cybersecurity capability domains rank below the 0,5 mark of utilisation, with no single score above 0,750. Figures 19 and 20 indicate to the water establishment which areas of cybersecurity can be improved upon and which are

functioning at the international best practice of 0,750; however, on this occasion none are. However, the overall maturity index is at 0,515, which is relatively good. The overall utilisation index score, on the other hand, is at 0,424, which is below the 0,500 (good) baseline. The survey results basically indicate that the ICS/SCADA cybersecurity practices are relatively good at 0,515 maturity, but that they are not being utilised as they should, which can leave the organisation vulnerable. Follow-up cyberresilience assessment interviews were conducted and the results are presented in the next section.

4.5.2 Interview findings

One participant was interviewed at this water establishment. As in the other three case studies, four main questions were asked, and the first question sought to determine the types of cybersecurity controls in place in the ICS environment. The second question sought to establish the perceived effectiveness and comprehensiveness scores for these controls. The results are shown in Table 13.

Table 13. Case 4 interview results

IT security controls (Level 1 cybersecurity practices)	**Effectiveness (Actual usage by employees)**	**Comprehensiveness (ICS security safeguards)**
Systems-driven physical security – biometric	0,900	0,900
Systems-driven physical security – closed circuit television (CCTV)	0,900	0,800
Human-driven physical security – manual	1,000	1,000
Human-driven physical security – tags	0,800	0,700
SCADA systems identity and access management	0,900	0,900
Supplier identity and access management	0,750	0,800
Supplier (supply chain) risk management	*0,000*	*0,000*
Anti-malware	0,600	0,900
Firewall	0,700	0,900
Overall	**0,728**	**0,767**

It can be seen from Table 13 that one security control was allocated effectiveness and comprehensiveness scores of zero. The participant indicated that currently there is a risk in that some subcontractors and SCADA software developers have system administrator and remote access rights to the network any time and from anywhere. In addition, the water establishment has no alert system, e.g. via text, to mitigate when and on what basis (service requests) the external service provider would be logging into their SCADA systems. Like many systems, there are event logs but with system administrator rights, these could be manipulated or even deleted. This is the only individual area of concern highlighted by the participant, as italicised in Table 13. In addition, Table 12 also revealed that the supply chain risk management capability score was much lower than the 0,500 (good) mark. Thus, the survey and interview scores align as far as risk posed by vendors is concerned.

The rest of the scores in Table 13 are quite high as indicated and the average scores also confirm good security controls at operational level. It should be recalled that the average utilisation score through the survey method was 0,424. The *utilisation index* determines the consistency and extent to which organisational cybersecurity practices are being used or how consistently and correctly implemented cybersecurity capabilities are applied. Thus, the average effectiveness score of 0,728 in Table 13 significantly contradicts the survey findings. The third interview question sought to establish the existence and configuration of the cybersecurity governance structure. It was found that the water entity has no formal SOC for the incidents management function. This is corroborated by the very low maturity and utilisation scores on the governance capability in the survey results. The authors are therefore inclined to lean more towards the survey findings as reflecting better ICS cybersecurity conditions in the water establishment. Thus, the effectiveness score should be around the 0,424 mark.

The STS classification of the interview results is shown in Table 14 to determine the balance in implementing technical and non-technical ICS security controls. The actors and environmental factors were derived from the interview transcript as some do not appear in Table 13.

Table 14. STS classification of ICS security controls

STS dimension	**STS domain**	**Categorised IT security controls**
Social	Organisational structure *(Functions)*	Human-driven physical security – manual Human-driven physical security – tags
	Actors *(People)*	SCADA team IT team Chief information officer Engineers
Technical	Technology *(Technical tools & resources)*	Anti-malware software SCADA systems identity and access management Supplier identity and access management Firewall Systems-driven physical security – biometric Systems-driven physical security – CCTV Supplier (supply chain) risk management
	Work activities *(Tasks)*	Vulnerability scans Auditing
Environmental		Suppliers Local government

Based on the STS classification in Table 14 and using effectiveness scores in Table 13, STS computations were made. Applying equation (1) and using effectiveness scores of *only* the scored security controls in Table 14 shows that the *overall social* X_b *= 0,900, technical* Y_b *= 0,679* and *environmental* Z_b *= indeterminate*. The environmental dimension is indeterminate because the supplier and government as identified from the interview were not allocated a score. Once again, the efficacy of the data collection methods utilised, and not the data analysis techniques, needs strengthening. As the *environmental dimension* (Z_b) is

indeterminate, JO cannot be computed using equation (2). Furthermore, the technical dimension (Y_b *= 0,679)* has a lower score than the social dimension. Further investigations of the water establishment's security controls are therefore required in the technical dimension to ensure closure of any security vulnerability gaps. This is in alignment with the lower survey results italicised in Table 12 where the average utilisation score is 0,424.

As indicated earlier, the third interview question found that the water establishment has no formal SOC for the incidents management function. This is corroborated by the very low maturity and utilisation scores on the governance capability in the survey results. As one of the bigger water establishments in Gauteng, this is concerning, although it was not established if the enterprise IT has a SOC. The fact that the ICS environment has no formalised processes and procedures to direct and control cybersecurity practices in their air-gapped environment is concerning on its own.

The final interview question sought to establish the types of cybersecurity incidents experienced so far. According to the interviewee, there have never been any major incidents up to this point in the ICS environment.

4.5.3 Conclusion

The water establishment has chosen an air-gapping strategy for securing their ICS/SCADA environment. It appears that having their own domain separate from that of enterprise IT has worked so far, as no major cybersecurity incidents have been reported. The interview results reveal one major concerning aspect, though, that corroborated the survey findings. The water establishment's SCADA service providers have the highest access privileges (system administrator profiles) to SCADA systems where they can remotely access the network any time and from anywhere. It is customary to have some, but not necessarily the highest, privileged access to do the necessary work, but the most concerning part of this is that the water establishment has no alert system, e.g. via text, to mitigate when and on what basis (service requests) the external service provider would be logging into their SCADA systems. On average, the water establishment's implemented ICS cybersecurity controls appear to be good/mature even though the STS assessment revealed that they are lacking in the technical dimension either in (additional security controls) implementation or utilisation.

4.6 Comparison of case studies

It is acknowledged that the water entities' profiles – human and financial resources, population sizes being provided with water services and reporting and governance structures – especially of the four case studies, are quite different. A comparison of the cybersecurity utilisation and maturity cannot simply be compared with each other as the water entities profiles are very different with different functions and resources. A comparison can be made in cases where

similar water organisations are tested, such as two large water boards or two municipalities of similar size and with similar resources. This research, however, targeted various organisations to gain insight on and get a perspective of different organisations in the sector.

The cybersecurity resilience comparisons in this section are therefore not based on their operational service delivery competence or lack thereof. Rather, the comparisons are based on the water entities' capability to utilise the fundamental best cybersecurity resilience practices despite the limited resources in comparison to peers. Table 15 shows the comparison of the cyberresilience capabilities of the four case studies.

Table 15. Cyberresilience comparison of the four case studies

Comparison factor	**Case study 1**	**Case study 2**	**Case study 3**	**Case study 4**	**Overall/mean**
Maturity of cybersecurity capabilities (Level 2 cybersecurity practices)	0,258	0,612	0,461	0,515	0,462
Normalised data value	*-1,363*	*1,008*	-0,003	0,358	
Utilisation of cybersecurity capabilities	0,292	0,517	0,414	0,424	0,412
Normalised data value	*-1,297*	*1,140*	0,024	0,133	
Effectiveness of cybersecurity controls (Level 1 cybersecurity practices)	0,598	0,600	0,492	0,728	0,605
Normalised data value	-0,067	-0,047	*-1,165*	*1,279*	
Comprehensiveness of cybersecurity controls	0,596	0,500	0,675	0,767	0,635
Normalised data value	-0,3387	*-1,183*	0,356	*1,166*	
Does formal cybersecurity governance structure exist?	No	Yes	Partially	No	Partially exists
Is ICS cybersecurity recognised as separate expertise area from enterprise IT security?	No	Yes	No	Yes	Partially recognised
Apart from human-driven physical security, are there ICS cybersecurity controls in place?	No	Very basic, and currently managed by enterprise IT	Very basic, and currently managed by enterprise IT	Yes	Basic to non-existent
Joint optimisation (Extent to which social, including human factors, technical and environmental security controls are balanced) before intervention efforts	0,117	0,231	Indeterminate	Indeterminate	Indeterminate
STS cybersecurity gaps?	Yes, likely within environmental dimension	Yes, likely within social dimension	Yes, likely within technical dimension	Yes, likely within technical dimension	Yes, within different STS dimensions

It is apparent from the statistical values in Table 15 that the sector is performing below average in terms of CI cybersecurity maturity practices (organisational implementors) at 0,462 and utilisation of security processes and procedures (organisational end-users) at 0,412. The overall comprehensiveness score of 0,635 is an indirect triangulation mechanism of the maturity score, and the overall effectiveness score of 0,605 is an indirect triangulation mechanism of the utilisation score. Effectively, the survey (maturity and utilisation indexes)

and interview findings (effectiveness and comprehensiveness indexes) should not deviate significantly. Unfortunately, they do deviate, as shown in Table 15. This can be explained through the normalised data values in italics in Table 13 where the mean and standard deviations are computed to show the data values causing the deviations.

This means that either more case studies (quantity) or more participants (quality) within the same case study organisations are required to minimise deviations from the statistical mean. The South African water sector's ability to prepare and plan for (anticipate), absorb (withstand), rapidly recover from (restore critical services) and successfully evolve from (adapt to) cyberattacks is at average. The maturity of cybersecurity capabilities (level 2 cybersecurity practices) of all four case studies can be visualised as a heat map as shown in Figure 21.

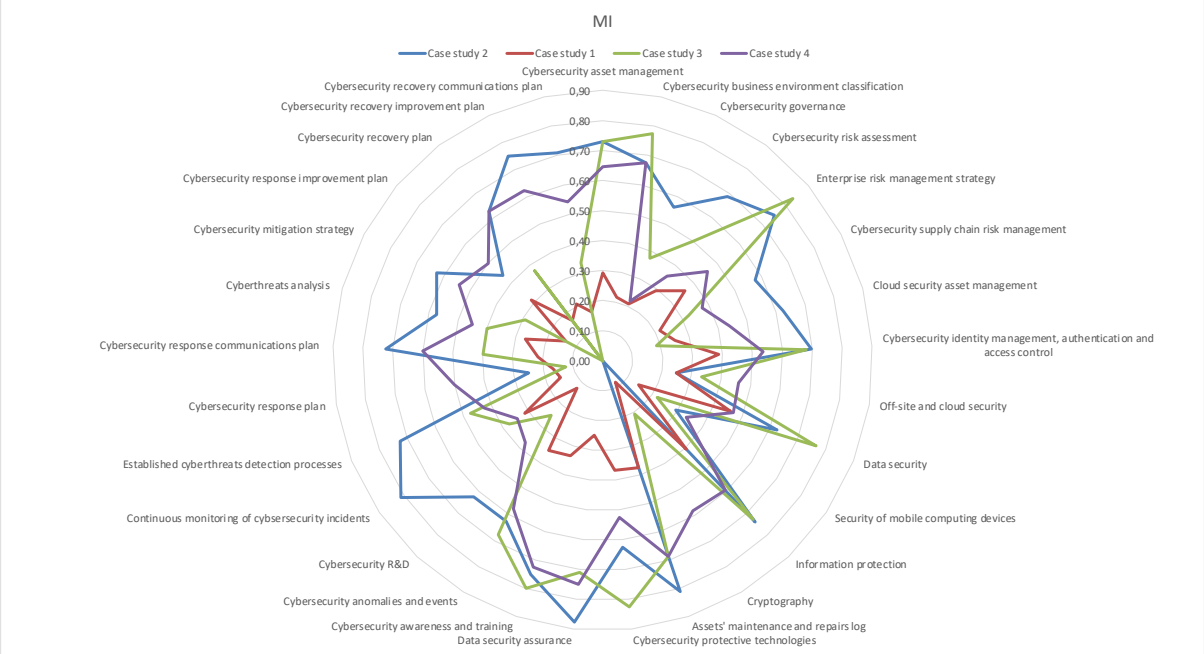

Figure 21. Water sector cybersecurity maturity

The levels of maturity in Figure 21 increase from the inner to the outer core. In other words, the more a case study occupies the inner core, the lower its level of cybersecurity capability maturity. In comparison with each other, Figure 21 shows that case study 1, which occupies mostly the inner core of the heat map, has lower cybersecurity capability maturity than all the other case studies. Case study 2 occupies the outer core mostly all around the heat map. Case study 3, on the other hand, occupies the outer core mostly on the north, south and east hemispheres and inner core on the west hemisphere of the heat map. Lastly, case study 4 shows higher cybersecurity capability maturity for practices on the north and south hemispheres and lower maturity on the east and west hemispheres.

The summarised results in Table 15 also indicate that a formalised cybersecurity governance structure only exists at case studies 2 and 3. However, case study 3 has only a basic to non-existent governance structure. Furthermore, case studies 2 and 4 recognise ICS cybersecurity as a separate profession with different security requirements and personnel skill sets than that of enterprise IT security. However, case study 2's enterprise IT teams are currently looking after some aspects of the ICS cybersecurity requirements; case study 4 has a fully functional and separate ICS cybersecurity team whose network domain is also air-gapped. The summarised results in Table 15 also indicate that the STS cybersecurity vulnerability gaps are more likely to exist in these organisations as they tend to emphasise one STS dimension at the expense of the others. This is crucial to attend to, as security is only as strong as its weakest link.

CI cybersecurity resilience assessments were conducted at four water establishments using the STS CAM. The assessments were conducted at level 2 (cybersecurity capabilities) cybersecurity practices with a survey questionnaire containing 140 questions based on the 140 CI cybersecurity capabilities developed by Malatji et al. (2021). The assessments required the maturity and utilisation indexes to be computed. Based on the summarised findings in Table 15, it can be concluded that the water sector's cybersecurity resilience is currently at average levels.

Only one and half of the case studies have a formalised cybersecurity governance structure in place. The rest address security concerns in an ad hoc manner, with few to no dedicated cybersecurity specialists available. In addition, only half of the water establishments recognise ICS cybersecurity as a separate profession with different security requirements and personnel skill sets than those of enterprise IT security.

Although the joint optimisation index – extent to which the social, including human factors, technical and environmental security controls are balanced – could not be computed due to the unavailability of the environmental dimension scores at two of the case studies, preliminary computations reveal some STS cybersecurity gaps. The summarised results in Table 15 indicate that the STS cybersecurity vulnerability gaps are more likely to exist in the case study organisations as they tend to emphasise one or two STS dimensions at the expense of the others. The overall findings are discussed in detail in the next section.

5. DISCUSSIONS OF WATER SECTOR CYBERRESILIENCE

5.1 Introduction

The recommended (international best practices) baseline level for cyberresilience operations is estimated to be about 0,750 (very good). However, each organisation must determine their own operational cyberresilience target based mainly on three aspects as recommended by NIST (2018): their security requirements, business objectives and technical environment/abilities. These factors will inform the organisation on how to work from this baseline to set goals, such as to first obtain a 0,400 or 40% maturity, then 0,500 (50% maturity) and so on. The baseline resilience level findings of South Africa's water sector are discussed in this section and the model used to conduct the resilience assessments is validated, including how this model – the socio-technical systems cyberresilience assessment model – can be continuously improved.

5.2 Water sector cyberresilience level

5.2.1 Enterprise IT security resilience

The water sector findings summarised in Table 15 indicate that at least 37,5% of the case study organisations have a structured approach to addressing enterprise IT security requirements through either a security standard, guideline, framework or any combination of these. Similarly, only 37,5% of the case study organisations have a formal cybersecurity governance structure in place to direct and control cybersecurity practices and human interactions. It is noted that the sector organisations that partially utilise a structured approach to addressing enterprise IT security concerns through either a security standard, guideline or framework only do this for governance as a regulatory compliance and statutory requirement as outlined in the Public Service Corporate Governance of Information and Communication Technology Policy Framework.

The findings also indicate that STS IT security vulnerability gaps are likely to exist as a result of the way in which the IT security controls (level 1 cybersecurity practices) are implemented. This opens socio-technical enterprise IT security gaps that could be exploited by attackers. It is acknowledged, however, that the STS scores were computed with incomplete data and are therefore merely indicative. The STS data elicitation method requires revision for more complete, reliable and valid data. Finally, the strongest theme that emerged regarding enterprise IT security practices is a shortage of IT security specialists and budget cuts across the IT departments.

5.2.2 ICS cybersecurity resilience

Although the findings in Table 15 indicate that there are currently partial ICS cybersecurity controls in place at 50% of the case study organisations, these are largely human-driven, but in certain instances there are systems-driven physical access control measures to plants. Moreover, where these systems-driven measures are in place, they are managed by the enterprise IT team. In other words, a formal ICS cybersecurity team only exists at 25% of the sector organisations studied. No formalised ICS cybersecurity practices exist at 75% of the sector organisations studied. The ICS/SCADA infrastructure at 75% of the case study organisations is therefore neither secure against nor resilient to any malicious cyberattacks and/or (un)intentional human errors.

5.2.3 Overall sector CI cyberresilience

Data indicates a below-average sector maturity of cybersecurity capabilities (level 2 cybersecurity practices) of 46,2%. The actual utilisation of the implemented cybersecurity capabilities is even worse at 41,2%, as indicated in Table 15. Similarly, the effectiveness of the cybersecurity controls (level 1 cybersecurity practices) in the sector is relatively good at 60,5%, and the comprehensiveness of these controls is above average at 63,5%. This means that the South African water sector's ability to prepare and plan for (anticipate), absorb (withstand), rapidly recover from (restore critical services) and successfully evolve from (adapt to) natural, human-made and autonomous adverse conditions, stresses, attacks and/or compromises is average.

The areas of concern that need immediate attention and improvement in both the enterprise IT and ICS environments appear to be under the maturity and utilisation elements of cybersecurity practices. It should be recalled that the maturity index measures how well and correctly cybersecurity practices are implemented by both the enterprise IT and ICS cybersecurity teams, whereas the utilisation index measures how consistently and correctly the cybersecurity practices implemented are being used by general employees. The general lack of formal cybersecurity governance structures and implementation frameworks at 62,5% of the sector organisations studied explains the below-average overall maturity and utilisation scores.

The findings also indicate that STS cybersecurity vulnerability gaps are likely to exist because of the way in which the security controls (level 1 cybersecurity practices) are implemented at organisational level. Essentially, STS principles state that no matter how mature, effective, comprehensive and utilised the cybersecurity controls may be, if a particular set of controls

between the social, technical and environmental dimensions is emphasised, the less emphasised one(s) will open a vulnerability gap that can be exploited by attackers. A balance therefore needs to be struck between the types of security controls implemented at organisational level and striving for higher levels of maturity, utilisation, effectiveness and comprehensiveness of the controls. Finally, inadequate availability of cybersecurity skills and budgetary constraints emerged strongly in all four case study organisations. The shortage of cybersecurity skills, in this case ICS cybersecurity skills, is also consistent with the assertion that the areas of cybersecurity concern in the sector appear to be in the maturity and utilisation of the cybersecurity practices.

5.3 Cyberresilience assessment model validation

Resilience assessments start with the definition of a CI's critical functions as a collective effect on the entire system's performance rather than individual components (Gisladottir et al., 2017). The STS CAM utilises five core elements (identify, protect, detect, respond and recover) and three STS elements (classify, optimise and mature) to define the critical functions of a CI's entire cyberresilience performance. It was found through the STS CAM deployment at the case study organisations that one of the most efficient methods to elicit near real-time data that reflects operational reality is through on-site and/or virtual workshops with *all* key stakeholders involved and for the *duration* required. The (subjective) self-reported cybersecurity maturity, utilisation, effectiveness and comprehensiveness scores attained in the case studies only hinted at what could be going on in the sector organisations. It is, however, acknowledged that workshops of this nature require time, top leadership commitment and financial and other resources.

The STS CAM operationalisation methods such as interviews and surveys should therefore be mixed with, if not replaced by, comprehensive workshops involving all key stakeholders. These workshops could take anything from a couple of days to a week or two, depending on various factors such as the size and topology configuration of the CI, number of key stakeholders involved and availability of financial and other resources. It is the authors' conclusion that the STS CAM has been validated through the case studies. Only its data elicitation techniques as described in this section require improvement to attain near real-time data that reflects operational reality.

The deployment of the assessment model in real-life settings through case studies serves as validation of the model. The overall sector resilience level (52,8%) indicates that the water sector's ability to prepare and plan for, absorb, rapidly recover from and successfully evolve from human-made and autonomous adverse conditions, stresses, attacks and/or

compromises is average. In particular, the areas of concern that need immediate attention and improvement in both the enterprise IT and ICS environments are in the maturity and utilisation elements of the cybersecurity practices. Consequently, the authors recommend a few steps to be taken to improve the cybersecurity resilience of the water sector in South Africa in the next section.

6. RECOMMENDATIONS

To improve the cybersecurity resilience of the water sector, the following recommendations are made:

- *Set up SOCs at larger sector organisations*. A formalised cybersecurity governance structure, such as a security operations centre to accommodate both the enterprise IT and ICS cybersecurity requirements, should be set up at larger sector organisations. At smaller water establishments, enterprise IT departments can be capacitated with additional ICS cybersecurity specialists as required, without the need for a formal SOC.
- *Adopt a cybersecurity standard, guideline or framework at organisational level*. A formal cybersecurity standard, guideline, framework or combination of these should be mandatory at all sector organisations to direct and control cybersecurity procedures and human interactions in a structured manner.
- *Commission specialised teams for enterprise IT security and ICS cybersecurity*. Dedicated teams should be established to address both enterprise IT security and ICS cybersecurity specialised areas. This will ensure that the required cybersecurity skills are acquired and suitable personnel recruited.
- *Conduct mandatory annual cybersecurity resilience assessments.* Annual cybersecurity resilience assessments should be conducted in the entire sector. A sector CSIRT should make this a mandatory requirement, through sector cybersecurity governance policies, for all sector organisations. Ideally, a sector CSIRT should facilitate this annual exercise not only to determine the level of resilience, but to encourage information and technology tools sharing, skills transfer, capacity building and collaboration within and outside the sector.

As future research, the authors recommend that the data elicitation techniques of the STS cybersecurity resilience assessment model be improved to attain near real-time data that reflects operational reality that is as accurate as possible. Time horizon and financial and human resources permitting, future research could also deploy the assessment model with 50% or more of the water sector population/actors participating in the study. This type of endeavour should eventually become an annual exercise to continuously improve the model while ascertaining the sector's level of cybersecurity resilience to strengthen safeguards.

7. CONCLUSIONS: WATER INFRASTRUCTURE CYBERSECURITY RESILIENCE

The aim of this study was to develop an STS cyberresilience assessment model, with the purpose of determining the resilience level of the water sector of South Africa. The CI cybersecurity capability framework, which is essentially the modified NIST CF, was adopted as the core framework of the cyberresilience assessment model. To quantify that CI owners/operators do not emphasise only the technical cybersecurity safeguards, the STS cybersecurity optimisation process overarched the core of the cyberresilience assessment model. Thus, two different frameworks were combined to develop the STS CAM. The aim of the study to develop an STS cyberresilience assessment model was therefore achieved.

The STS CAM was deployed in real-life settings through case studies. The case organisations were the water sector CI owners and operators in the public sector. The overall findings of the STS CAM deployment are that the cyberresilience of the water sector is average in both the enterprise IT and ICS environments. However, the results reflect more the enterprise IT security than ICS cybersecurity performance, as fewer security practices were assessed in the ICS environment in all case studies. Thus, a pattern emerged from the case studies that thought of cybersecurity as something that only concerns, and should be the purview of, enterprise IT.

It is for this reason that formalised SOCs to accommodate both the enterprise IT and ICS cybersecurity specialised teams should be established at larger water establishments. The teams need not be very big; the size can be determined by a water establishment's security requirements, business objectives and technical abilities. Thus, smaller water establishments may not necessarily even require the establishment of a SOC. One or two cybersecurity specialists per IT and ICS environments could be adequate, depending on the requirements, and both governed within the enterprise IT department. A formal security programme in this regard can be initiated by adopting the CI cybersecurity capability framework and conducting periodic resilience assessments through the STS CAM.

Lessons learnt from the deployment of the STS CAM is that the best method to elicit near real-time data that reflects reality on the ground is on-site/virtual workshops involving all key stakeholders and for the duration required. The (subjective) self-reported security maturity, utilisation, effectiveness and comprehensiveness scores only provide a hint as to what could be going on in the organisation. It is, however, acknowledged that workshops of this nature require time, top leadership commitment and financial and other resources. However,

investment in cybersecurity programmes should no longer be a side risk. After all, cyberresilience can only be successfully realised through meaningful partnerships and continual collaborations among all key stakeholders in the sector. It is a strategic requirement that should be driven by boards of directors and executive management of every sector organisation.

REFERENCES

Alexandru, U. (2016). Evolution of Scada systems. *Bulletin of the Transilvania University of Brasov. Engineering Sciences. Series I.*, *9*(58), 63-68.

Annarelli, A., Nonino, F., & Palombi, G. (2020). Understanding the management of cyber resilient systems. *Computers & Industrial Engineering*, *149*, 106829. https://doi.org/10.1016/j.cie.2020.106829.

Arghandeh, R., Von Meier, A., Mehrmanesh, L., & Mili, L. (2016). On the definition of cyberphysical resilience in power systems. *Renewable and Sustainable Energy Reviews*, *58*, 1060-1069. https://doi.org/10.1016/j.rser.2015.12.193.

Ayyub, B. M. (2014). Systems resilience for multihazard environments: Definition, metrics, and valuation for decision making. *Risk Analysis, 34*(2), 340-355. https://doi.org/10.1111/risa.12093.

Azadeh, A., Salehi, V., Arvan, M., & Dolatkhah, M. (2014). Assessment of resilience engineering factors in high-risk environments by fuzzy cognitive maps. *Safety Science*, *68*, 99-107. https://doi.org/10.1016/j.ssci.2014.03.004.

Babiceanu, R. F., & Seker, R. (2019). Cyber resilience protection for industrial internet of things: A software-defined networking approach. *Computers in Industry*, *104*, 47-58. https://doi.org/10.1016/j.compind.2018.10.004.

Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber resilience – Fundamentals for a definition. In Á. Rocha, A. M. Correia, S. Costanzo, & L. P. Reis (Eds.), *New contributions in information systems and technologies: Advances in intelligent systems and computing* (pp. 311-316). https://doi.org/10.1007/978-3-319-16486-1_31.

Bodeau, D., & Graubart, R. (2016). Cyber resilience metrics: Key observations. Retrieved 24 May 2021, from https://web.archive.org/web/20210524152054/https://www.mitre.org/sites/default/files/publications/16-0779-cyber-resilience-metrics-key-observations.pdf.

Bodeau, D., & Graubart, R. (2017). The MITRE Corporation: Cyber resiliency design principles. Retrieved 8 March 2021, from https://web.archive.org/web/20201217140635/https://www.mitre.org/sites/default/files/publications/PR 17-0103 Cyber Resiliency Design Principles MTR17001.pdf.

Bodeau, D. J., Graubart, R. D., Heinbockel, W. J., & Laderman, E. (2015). The MITRE Corporation: Cyber resiliency engineering aid – the updated cyber resiliency engineering framework and guidance on applying cyber resiliency techniques. Retrieved 13 March 2021, from https://web.archive.org/web/20200621024647/https://www.mitre.org/publications/technical-papers/cyber-resiliency-engineering-aid-the-updated-cyber-resiliency.

Butler, D., Farmani, R., Fu, G., Ward, S., Diao, K., & Astaraie-Imani, M. (2014). A new approach to urban water management: Safe and sure. *Procedia Engineering*, *89*, 347-354. https://doi.org/10.1016/j.proeng.2014.11.198.

Campbell, T. (2016). *Practical information security management: A complete guide to planning and implementation.* New York, NY: Apress.

Caralli, R. A., Allen, J. H., Curtis, D. P., White, D. W., Young, L. R., & Mehravari, N. (2016). CERT® resilience management model, version 1.2. Retrieved 10 March 2021, from https://web.archive.org/web/20210119232025/https://resources.sei.cmu.edu/asset_files/Handbook/2016_002_001_514462.pdf.

Carayon, P., Hancock, P., Leveson, N., Noy, I., Sznelwa, L., & Van Hootegem, G. (2015). Advancing a sociotechnical systems approach to workplace safety – developing the conceptual framework. *Ergonomics*, *58*(4), 548-564.

Carías, J., Labaka, L., Sarriegi, J., & Hernantes, J. (2019). Defining a cyber resilience investment strategy in an Industrial Internet of Things context. *Sensors*, *19*(1), 138. https://doi.org/10.3390/s19010138.

Carías, J. F., Arrizabalaga, S., Labaka, L., & Hernantes, J. (2020). Cyber resilience progression model. *Applied Sciences*, *10*(21), 7393. https://doi.org/10.3390/app10217393.

Chaves, A., Rice, M., Dunlap, S., & Pecarina, J. (2017). Improving the cyber resilience of industrial control systems. *International Journal of Critical Infrastructure Protection*, *17*, 30-48. https://doi.org/10.1016/j.ijcip.2017.03.005.

Chen, S. P., & Redar, J. M. (2014). Ageing workforce knowledge management and transactional & transformational leadership: A socio-technical systems framework and a Norwegian case study. *International Journal of Business and Social Science*, *5*(5), 11-21.

Clark, R. M., & Hakim, S. (2014). Securing water and wastewater systems: Global experiences. In R. M. Clark & S. Hakim (Eds.), *Securing water and wastewater systems: Protecting critical infrastructure*. https://doi.org/10.1007/978-3-319-01092-2.

Clédel, T., Cuppens, N., Cuppens, F., & Dagnas, R. (2020). Resilience properties and metrics: How far have we gone? *Journal of Surveillance, Security and Safety*, *1*, 119-139. https://doi.org/10.20517/jsss.2020.08.

Collier, Z. A., Linkov, I., DiMase, D., Walters, S., Tehranipoor, M., & Lambert, J. H. (2014). Cybersecurity standards: Managing risk and creating resilience. *Computer*, *47*(9), 70-76. https://doi.org/10.1109/MC.2013.448.

Collier, Z. A., Panwar, M., Ganin, A. A., Kott, A., & Linkov, I. (2016). Security metrics in industrial control systems. In E. J. M. Colbert & A. Kott (Eds.), *Cyber-security of SCADA and other industrial control systems* (pp. 167-185). Cham, Switzerland: Springer.

Davis, M. C., Challenger, R., Jayewardene, D. N. W., & Clegg, C. (2014). Advancing socio-technical systems thinking: A call for bravery. *Applied Ergonomics*, *45*(2A), 171-180.

De Bruin, R., & Von Solms, S. H. (2016). Cybersecurity governance: How can we measure it? *Proceedings of the 11th IST-Africa Week Conference.* 11-13 May, Durban, South Africa: IEEE.

Dessavreand, D. G., & Ramirez-Marquez, J. E. (2015). Computational techniques for the approximation of total system resilience. In L. Podofillini, B. Sudret, B. Stojadinovic, E. Zio, & W. Kröger (Eds.), *Safety and reliability of complex engineered systems* (pp. 145-150). Boca Raton, Florida: CRC Press.

Dickson, F., & Goodwin, P. (2020). White Paper: Five key technologies for enabling a cyber-resilience framework. Retrieved 3 March 2021, from https://web.archive.org/web/20200526204459/https://www.ibm.com/downloads/cas/YBDGKDXO.

DiMase, D., Collier, Z. A., Heffner, K., & Linkov, I. (2015). Systems engineering framework for cyber physical security and resilience. *Environment Systems and Decisions*, *35*(2), 291-300. https://doi.org/10.1007/s10669-015-9540-y.

Donaldson, S. E., Siegel, S. G., Williams, C. K., & Aslam, A. (2018). *Enterprise cybersecurity study guide: How to build a successful cyberdefense program against advanced threats.* New York, NY: Apress.

Franciosi, C., Voisin, A., Miranda, S., Riemma, S., & Iung, B. (2020). Measuring maintenance impacts on sustainability of manufacturing industries: From a systematic literature review to a framework proposal. *Journal of Cleaner Production*, *260*, 121065. https://doi.org/10.1016/j.jclepro.2020.121065.

Francis, R., & Bekera, B. (2014). A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliability Engineering & System Safety*, *121*, 90-103. https://doi.org/10.1016/j.ress.2013.07.004.

Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2017). Multicriteria decision framework for cybersecurity risk assessment and management. *Risk Analysis*, *40*(4). https://doi.org/10.1111/risa.12891.

Gasser, P., Lustenberger, P., Cinelli, M., Kim, W., Spada, M., Burgherr, P., … Sun, T. (2019). A review on resilience assessment of energy systems. *Sustainable and Resilient Infrastructure*. https://doi.org/10.1080/23789689.2019.1610600.

Gisladottir, V., Ganin, A. A., Keisler, J. M., Kepner, J. & Linkov, I. (2017). Resilience of cyber systems with over- and underregulation. *Risk Analysis*, 37(9), 1644-1651. https://doi.org/10.1111/risa.12729.

Hahn, A. (2016). Operational technology and information technology in industrial control systems. In E. J. M. Colbert & A. Kott (Eds.), *Cyber-security of SCADA and other industrial control systems: Advances in information security, vol. 66* (pp. 51-68). https://doi.org/10.1007/978-3-319-32125-7_4.

Haimes, Y. Y. (2009). On the definition of resilience in systems. *Risk Analysis*, *29*(4), 498-501. https://doi.org/10.1111/j.1539-6924.2009.01216.x.

Hale, A., & Heijer, T. (2006). Defining resilience. In E. Hollnagel, D. Woods, & N. Leveson (Eds.), *Resilience engineering: Concepts and precepts* (pp. 35-40). Hampshire, United Kingdom: Ashgate.

Hardison, T. (2018). ISACA – Building a strong security posture begins with assessment. *ISACA Journal*, *3*, 1-5.

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, *58*(102726).

Hausken, K. (2020). Cyber resilience in firms, organizations and societies. *Internet of Things*, *11*, 100204. https://doi.org/10.1016/j.iot.2020.100204.

Heinimann, H. R., & Hatfield, K. (2017). Infrastructure resilience assessment, management and governance – State and perspectives. In I. Linkov & J. M. Palma-Oliveira (Eds.), *Resilience and risk, NATO science for peace and security series C: Environmental security* (pp. 147-185). https://doi.org/10.1007/978-94-024-1123-2_5.

Imani, M., & Hajializadeh, D. (2020). A resilience assessment framework for critical infrastructure networks' interdependencies. *Water Science & Technology*, *81*(7), 1420-1431. https://doi.org/10.2166/wst.2019.367.

ISO. (2021). Technical committees: ISO/TC 292 Security and resilience. Retrieved 10 March2021, from https://web.archive.org/web/20210126091359/https://www.iso.org/committee/5259148.html.

Jackson, S. (2015). Overview of resilience and theme issue on the resilience of systems. *Insight*, *18*(1), 7-9. https://doi.org/10.1002/inst.12001.

Janke, R., Tryby, M. & Clark, R. M. (2014). Protecting water supply critical infrastructure: An overview. In R. M. Clark & S. Hakim (Eds.), *Securing water and wastewater systems: Protecting critical infrastructure* (pp. 29-85). Cham: Springer International.

Krotofil, M., Kursawe, K., & Gollmann, D. (2019). Securing industrial control systems. In C. Alcaraz (Ed.), *Security and privacy trends in the Industrial Internet of Things: Advanced sciences and technologies for security applications* (pp. 3-26). https://doi.org/10.1007/978-3-030-12330-7_1.

Lees, M. J., Crawford, M., & Jansen, C. (2018). Towards industrial cybersecurity resilience of multinational corporations. *IFAC PapersOnLine*, *51030*, 756-761. https://doi.org/10.1016/j.ifacol.2018.11.201.

Linkov (A). I., & Trump, B. D. (2019). Risk and resilience: Similarities and differences. In *The science and practice of resilience. Risk, systems and decisions.* (pp. 3-7). Cham, Switzerland: Springer.

Linkov (A). I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Le Kott, A. (2013). Resilience metrics for cyber systems. *Environ Syst Decis*, *33*, 71-476. https://doi.org/10.1007/s10669-013-9485-y.

Linkov, I., & Kott, A. (2019). Fundamental concepts of cyber resilience: Introduction and overview. In A. Kott & I. Linkov (Eds.), *Resilience of systems and networks. Risk, systems and decisions.* (pp. 1-25). https://doi.org/10.1007/978-3-319-77492-3_1.

Linkov, I., Eisenberg, D. A., Bates, M. E., Chang, D., Convertino, M., Allen, J. H., … Seager, T. P. (2013). Measurable resilience for actionable policy. *Environmental Science & Technology*, *47*, 10108−10110. https://doi.org/10.1021/es403443n.

Malatji, M., Marnewick, A., & Von Solms, S. (2020). Validation of a socio-technical management process for optimising cybersecurity practices. *Computers and Security*, *95*. https://doi.org/10.1016/j.cose.2020.101846.

Malatji, M., Marnewick, A. L. & Von Solms, S. (2021). Cybersecurity capabilities for critical infrastructure resilience. *Information and Computer Security*, *X*(Y), xxx - yyy.

Mbanaso, U. M., Abrahams, L., & Apene, O. Z. (2019). Conceptual design of a cybersecurity resilience maturity measurement (CRMM) framework. *African Journal of Information and Communication*, *23*, 1-26. https://doi.org/10.23962/10539/27535.

Mohebbi, S., Zhang, Q., Wells, E. C., Zhao, T., Nguyen, H., Li, M., … Ou, X. (2020). Cyber-physical-social interdependencies and organizational resilience: A review of water, transportation, and cyber infrastructure systems and processes. *Sustainable Cities and Society*, *62*, 102327. https://doi.org/10.1016/j.scs.2020.102327.

Mumford, E. (2006). The story of socio-technical design: Reflections on its successes, failures and potential. *Information Systems Journal*, *16*(4), 317-342.

Naden, C. (2021). International standard for crime prevention through environmental design (CPTED) just published. Retrieved 10 March 2021, from https://web.archive.org/web/20210204191405/https://www.iso.org/news/ref2620.html.

Nan, C., & Sansavini, G. (2017). A quantitative method for assessing resilience of interdependent infrastructures. *Reliability Engineering and System Safety*, *157*, 35-53. https://doi.org/10.1016/j.ress.2016.08.013.

National Academy of Sciences. (2012). Disaster resilience: A national imperative. Retrieved 15 May 2021, from https://www.nap.edu/catalog/13457/disaster-resilience-a-national-imperative.

NIST. (2015). Guide to industrial control systems (ICS) Security, Revision 2. Retrieved 18 July2020, from https://web.archive.org/web/20201116222442/https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final.

NIST. (2018). Framework for improving critical infrastructure cybersecurity, version 1.1. Retrieved 18 July 2010, from https://web.archive.org/web/20201122005055/https://www.nist.gov/cyberframework.

Ouyang, M., Dueñas-Osorio, L., & Min, X. (2012). A three-stage resilience analysis framework for urban infrastructure systems. *Structural Safety*, *36-37*, 23-31. https://doi.org/10.1016/j.strusafe.2011.12.004.

Panguluri, S., William, P. R. J., & Clark, R. M. (2004). Cyber threats and IT/SCADAsystem vulnerability. In L. W. Mays (Ed.), *Water supply systems security* (pp. 5.1-5.18). New York: McGraw-Hill.

Panteli, M., & Mancarella, P. (2015). The grid: Stronger, bigger, smarter? Presenting a conceptual framework of power system resilience. *IEEE Power and Energy Magazine*, *13*((3)), 58-66.

Pescatore, J. (2020). How to optimise security operations in the cloud through the lens of the NIST Framework. In SANS Institute (Ed.), *SANS: Practical guide to security in the AWS cloud, Volume I.* (pp. 18-36). SANS Institute.

Redman, C. L. (2014). Should sustainability and resilience be combined or remain distinct pursuits? *Ecology and Society*, *19*(2), 37. https://doi.org/10.5751/ES-06390-190237.

Rehak, D., & Hromada, M. (2018). Critical infrastructure system. In T. Nakamura (Ed.), *System of system failures* (pp. 75-93). https://doi.org/10.5772/intechopen.70446.

Rehak, D., Senovsky, P., Hromada, M., & Lovecek, T. (2019). Complex approach to assessing resilience of critical infrastructure elements. *International Journal of Critical Infrastructure Protection*, *25*, 125-138. https://doi.org/10.1016/j.ijcip.2019.03.003.

Rieger, C. G. (2014). Resilient control systems: Practical metrics basis for defining mission impact. In C. G. Rieger (Ed.), *Proceedings of the 2014 7th International Symposium on Resilient Control Systems*. https://doi.org/10.1109/ISRCS.2014.6900108.

Roege, P. E., Collier, Z. A., Chevardin, V., Chouinard, P., Florin, M., Lambert, J. H., … Todorovic, B. (2017). Bridging the gap from cyber security to resilience. In I. Linkov & J. M. Palma-Oliveira (Eds.), *Resilience and risk* (pp. 383-414). https://doi.org/10.1007/978-94-024-1123-2_14.

South Africa. (2015). National Cybersecurity Policy Framework (NCPF). Retrieved 10 April 2020, from https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf.

Stellios, I., Kotzanikolaou, P., & Psarakis, M. (2019). Advanced persistent threats and zero-day exploits in Industrial Internet of Things. In C. Alcaraz (Ed.), *Security and privacy trends in the Industrial Internet of Things: Advanced sciences and technologies for security applications* (pp. 47-68). https://doi.org/10.1007/978-3-030-12330-7_3.

Sullivan, D., Luiijf, E., & Colbert, E. J. M. (2016). Components of industrial control systems. In E. Colbert & A. Kott (Eds.), *Cyber-security of SCADA and other industrial control systems: Advances in information security, vol 66* (pp. 15-28). https://doi.org/10.1007/978-3-319-32125-7_2.

Susskind, N. G. (2014). Cybersecurity compliance and risk management strategies: What directors, officers and managers need to know. *NYU Journal of Law & Business*, *11*(5), 73-76.

Thorisson, H., Lambert, J. H., Cardenas, J. J., & Linkov, I. (2017). Resilience analytics with application to power grid of a developing region. *Risk Analysis*, *37*(7), 1268-1286. https://doi.org/10.1111/risa.12711.

Tonhauser, M., & Ristvej, J. (2019). Disruptive acts in cyberspace, steps to improve cyber resilience at national level. *Transportation Research Procedia*, *40*, 1591-1596. https://doi.org/10.1016/j.trpro.2019.07.220.

Troyer, L. (2017). Expanding sociotechnical systems theory through the trans-disciplinary lens of complexity theory. In J. Kahlen, S. Flumerfelt, & A. Alves (Eds.), *Transdisciplinary perspectives on complex systems* (pp. 177-192). Cham, Switzerland: Springer.

Vugrin, E. D., Warren, D. E., & Ehlen, M. A. (2011). A resilience assessment framework for infrastructure and economic systems: Quantitative and qualitative resilience analysis of petrochemical supply chains to a hurricane. *Process Safety Progress*, *30*(3), 280-290. https://doi.org/10.1002/prs.10437.

Walker, G. H., Stanton, N. A., Jenkins, D., Salmon, P., Young, M., & Aujla, A. (2007). Sociotechnical theory and NEC system design. In D. Harris (Ed.), *Engineering psychology and cognitive ergonomics* (pp. 619-628). Berlin, Germany: Springer-Verlag.

Washington, M., & Hacker, M. (2000). Joint optimisation system element: The application of joint optimization. *Measuring Business Excellence*, *4*(4), 18-24.

WEF. (2020). Cyber resilience in the electricity ecosystem: Playbook for boards and cybersecurity Officers. Retrieved 8 March 2021, from https://web.archive.org/web/20210202173756/https://www.weforum.org/reports/cyber-resilience-in-the-electricity-ecosystem-playbook-for-boards-and-cybersecurity-officers/.

Wu, P. P., Fookes, C., Pitchforth, J., & Mengersen, K. (2015). A framework for model integration and holistic modelling of socio-technical systems. *Decision Support Systems*, *71*, 14-27.

Young, W., & Leveson, N. G. (2014). An integrated approach to safety and security based on systems theory. *Communications of the ACM*, *57*(2), 31-35. https://doi.org/10.1145/2556938.

APPENDIX A: WATER SECTOR CYBERSECURITY RESILIENCE ASSESSMENT

Dear Information & Cybersecurity Practitioner,

The University of Johannesburg would like to invite you to participate in a research survey being carried out as part of the Water Research Commission (WRC)'s project to determine cybersecurity governance in the water sector.

Background and purpose
Like other sectors in South Africa, the water sector needs to address the sector-specific cybersecurity risks proactively and effectively within the guidelines of the National Cybersecurity Policy Framework (NCPF). The NCPF is the Cabinet-approved national cybersecurity strategy of South Africa. To effectively and proactively address sector-specific cyberrisks, a legislative and policy framework, resilience and risk posture, governance framework as well as education and training materials are required. By answering all questions to the best of your ability, you will be assisting the country, water and sanitation sector, your organisation, and individual colleagues in fighting cybercrime and staying resilient.

Case Study Sample
The study is aimed at any information and cybersecurity practitioners and researchers 18 years old and above in the water and sanitation sector of South Africa. You must have been active in this field for at least 3 years. Your responses are important in helping the entire water and sanitation sector determine its level of resilience and risk posture.

Autonomy, Non-maleficence, Beneficence, and Justice
Your decision to participate in the study is completely voluntary and you can withdraw anytime without giving reasons. Any responses you provide will be anonymous and treated in the strictest confidence. The study is only interested in your computer security experiences in the water sector. Your responses will therefore only be used as the main dataset for the WRC sponsored research study. All reasonable endeavours were made to ensure that no harm, now and into the future, may be caused to respondents because of their responses. Absolute anonymity and confidentiality are therefore guaranteed since your names and contact details are not required anywhere in the study. The management and analysis of the data gathered will also comply with the relevant data protection legislations to guarantee privacy. Informed consent is assumed once a person has read and understood all the above and continued to complete the survey.

Contact details for further information
If you have any questions or would like further information, please do not hesitate to contact the project leader on +2711 559 1735 or amarnewick@uj.ac.za.

Thank you for your help.

Regards,

Dr. Masike Malatji | Prof. Annlizé L. Marnewick | Prof. Suné von Solms

Section 2: Survey instructions

The survey questionnaire should take you approximately 60 minutes to complete. Try to complete the questionnaire at your most convenient time and without disturbance. The survey questionnaire contains two main sections: Biographical information and structured cybersecurity assessment questions sections. The biographical information is used to evaluate your suitability to complete the survey against the study sample criteria. The structured cybersecurity assessment questions section, on the other hand, contains about 29 close-ended questions. Each of the 29 close-ended questions corresponds to one of the 29 level 2 cybersecurity practices (cybersecurity capability domains) of the study. For each of the 29 questions, two object characteristics need to be measured. These are the 'maturity' and 'utilisation' characteristics or indexes. The 'object' in object characteristics refers to 140 cybersecurity capabilities (required process and technology results) associated with the 29 cybersecurity capability domains. The *maturity index* determines the degree to which organisational cybersecurity practices have been formalised and optimised (how well and correctly a cybersecurity capability is implemented), and the *utilisation index* determines the consistency and extent to which organisational cybersecurity practices are being used (how consistently and correctly an implemented cybersecurity capability is applied). From the two indexes, the *overall cybersecurity assessment index* will be computed to determine the overall organisational/sector resilience and risk posture and areas requiring immediate improvement.

It is important to measure both 'maturity' and 'utilisation' indexes because a cybersecurity capability domain can have several of its cybersecurity capabilities present and utilised; however, if they are not correctly configured (i.e., matured), they can be ineffective and/or neutralised by a persistent cyberattacker." I hope that you will find the questions insightful and enjoyable by selecting, to the best of your ability, either: **N/A** (not applicable); **0.00** (absent); **0.25** (weak); **0.50** (good); **0.75** (very good); **1.00** (excellent).

Section 3: Biographical Information

This information will only be used to ensure that you meet the case study sample selection criteria.

My years of experience in the information and cybersecurity domain are:	< 3 years	3-5 years	6-14 years	15-35 years	> 35 years
My formal qualifications are:	Security certificate/s	Bachelor's degree	Masters/ Doctorate	Certificate/s + Bachelor's	Certificate/s + Masters/ Doctorate
I am engaged in information and cybersecurity work as a:	Practitioner	Researcher			

Sections 4: Structured Cybersecurity Assessment Questions

Please provide your expert judgement/opinion by allocating a score to each 'object' (cybersecurity capability) according to your experiences in the organisation.

IDENTIFY	**No.**	
	1	**Do you perform cybersecurity asset management activities according to established policy, processes, and procedures?**
	1.1	Identification and documentation of (all) systems and physical devices in the organisation
	1.2	Identification and documentation of (all) software platforms and applications in the organisation
	1.3	Mapping of organisational communication and data flows
	1.4	Cataloguing of external information systems
	1.5	Prioritisation of resources (e.g., personnel, data, hardware, software, devices, and time) based on business value, classification, and criticality
	1.6	Establishment of cybersecurity roles and responsibilities for the entire organisation's workforce and third-party stakeholders (e.g., customers, vendors, partners)
	2	**Do you perform cybersecurity business environment classification?**
	2.1	Identification and communication of the organisation's role in the supply chain.
	2.2	Identification and communication of the organisation's critical infrastructure place and sector.
	2.3	Establishment and communication of priorities for organisational mission, objectives, and activities.
	2.4	Establishment of dependencies and critical functions for delivery of critical services.
	2.5	Establishment of resilience requirements to support delivery of critical services for all operating states (e.g., normal operations, under duress/attack, during recovery).

	3	**Do you perform cybersecurity governance activities according to established policy, processes, and procedures?**
	3.1	Establishment and communication of the organisational cybersecurity policy.
	3.2	Coordination of cybersecurity roles and responsibilities in alignment with internal roles and external partners.
	3.3	Understanding and management of cybersecurity legal and regulatory requirements, including privacy and civil liberties obligations.
	3.4	Assurance that governance and risk management processes address cybersecurity risks.
	4	**Do you perform cybersecurity risk assessments activities according to established policy, processes and procedures?**
	4.1	Identification and documentation of assets vulnerabilities.
	4.2	Enrolment and receipt of cyberthreat intelligence from information sharing forums and sources.
	4.3	Identification and documentation of both internal and external threats.
	4.4	Identification of potential business impacts and likelihoods.
	4.5	Determination of risk posture from internal and external threats, vulnerabilities, likelihoods, and impacts.
	4.6	Identification and prioritisation of risk responses.
	5	**Do you have an enterprise risk management strategy that incorporates cybersecurity risks?**
	5.1	Establishment and management of risk management processes that are agreed to by all relevant organisational stakeholders.
	5.2	Determination of the organisational risk tolerance that is clearly expressed enterprise wide.
	5.3	Assurance that the organisation’s determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis.
	6	**Do you perform cybersecurity supply chain risk management activities according to established policy,**

		processes and procedures?
	6.1	Identification, establishment, assessment, and management of cyber supply chain risk management processes that are agreed to by all relevant organisational stakeholders.
	6.2	Identification, prioritisation and assessment of suppliers and third-party partners of information systems, components, and services using a cyber supply chain risk assessment process.
	6.3	Implementation of appropriate measures designed to meet the objectives of an organisation's cybersecurity program and cyber supply chain risk management plan through contracts with suppliers and third-party partners.
	6.4	Routine assessments of suppliers and third-party partners using audits, test results, or other forms of evaluations to confirm that they are meeting contractual obligations.
	6.5	Conductance of response and recovery planning and testing with suppliers and third-party partners.
	7	**Do you perform cloud security asset management activities according to established policy, processes, and procedures?**
	7.1	Regular maintenance and updating of a complete inventory of assets located at cloud service providers and/or their geographical locations and usage over time. Ownership of these is also assigned by defined roles and responsibilities, where applicable.
	7.2	Automated equipment identification is used as a method of connection authentication. Location-aware technologies are also used to validate connection authentication integrity based on known equipment location.
PROTECT	**8**	**Do you perform cybersecurity identity management, authentication, and access control activities according to established policy, processes, and procedures?**
	8.1	Issuance, management, verification, revocation and auditing of identities and credentials for authorised devices, users, and processes.
	8.2	Management and protection of physical access to assets.

	8.3	Management of remote access to assets and information systems.
	8.4	Management of access permissions and authorisations, incorporating the principles of least privilege and separation of duties.
	8.5	Protection of network integrity (e.g., network segmentation and segregation).
	8.6	Validation of identities bound to credentials and asserted in interactions.
	8.7	Authentication of assets, devices, and users at the level of risk commensurate with the transaction being performed.
	9	**Do you perform off-site and cloud security activities according to established policy, processes, and procedures?**
	9.1	Establishment and implementation of cloud security policies, processes, and procedures.
	9.2	Establishment and enforcement of off-site authorisation policies and procedures to facilitate authorisation for relocation and/or transfer of assets (e.g., data, equipment, software and hardware) to an offsite premise such as at a cloud service provider.
	9.3	Establishment and enforcement of procedures for the secure disposal of equipment used outside the organisation's premises are facilitated through appropriate policies and procedures. These policies and procedures include a data destruction process that renders recovery of information impossible.
	10	**Do you carry out data security activities according to established policy, processes, and procedures?**
	10.1	Protection of data-at-rest.
	10.2	Protection of data-in-transit.
	10.3	Formal management of assets throughout removal, transfers, and disposition.
	10.4	Assurance of adequate capacity for maintenance of data availability.
	10.5	Implementation of protection against data leaks.
	10.6	Verification of software, firmware, and information integrity through integrity checking mechanisms.

	10.7	The development and testing environment(s) are separate from the production environment.
	10.8	Verification of hardware integrity through integrity checking mechanisms.
	11	**Do you actively manage security of mobile computing devices according to established policy, processes, and procedures?**
	11.1	Anti-malware: A vendor's cybersecurity awareness training includes anti-malware awareness training specific to mobile devices.
	11.2	Application stores: Mobile devices storing or accessing vendor managed data are managed through an acceptable and approved documented list of (software) application stores.
	11.3	Approved applications: Installation or downloading of mobile applications not obtained through an acceptable and approved documented list of application stores are prohibited via policy.
	11.4	Approved software for Bring Your Own Device (BYOD): The approved application stores, mobile applications, application extensions, and plugins that may be utilised for BYOD purposes are supported by a clear BYOD policy and awareness training in the organisation.
	11.5	Awareness and training: A documented mobile device policy that includes acceptable requirements and usage for all mobile devices, including BYOD, has been provided for by the vendor. The policy also has a clear definition of what constitute a mobile device, including BYOD, and is regularly communicated through the organisation's security awareness and training program.
	11.6	Cloud-based services: BYOD and/or mobile device activities relating to company business data storage and usage at cloud service providers obtain organisational pre-approval first.
	11.7	Compatibility: An application validation process to test for mobile devices, application compatibility issues, and operating systems has been documented in the organisation.
	11.8	Device eligibility: The device and eligibility requirements to allow for BYOD usage is clearly defined in the BYOD policy.

	11.9	Device inventory: All mobile devices used to store and access company data have been inventoried and such an inventory list is regularly updated. For example, the inventory procedure records all changes to the status of BYOD or mobile devices such as to whom the mobile device is assigned or approved for usage (BYOD), patch levels, operating system, and lost or decommissioned status.
	11.10	Device management: All mobile devices or approved BYOD permitted to store, process, or transmit customer data are managed through a centralised mobile device management system.
	11.11	Encryption: A mobile device policy enforced through technology controls has been put in place to ensure encryption of either the entire device or for data identified as sensitive on all mobile devices.
	11.12	Jailbreaking and rooting: A mobile device policy enforced through technology controls has been put in place to prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting).
	11.13	Legal: Simple language has been used in the the BYOD policy to outline the privacy expectations, e-discovery, requirements for litigation and legal holds, and loss of non-company data in the event that a wipe of the device is required.
	11.14	Lockout screen: An automatic lockout screen setting has been configured on all approved BYOD and/or assigned mobile devices, and the requirement is enforced through technical controls.
	11.15	Operating systems: Organisation-wide control processes are used to manage changes to mobile device applications, operating systems, and/or patch levels.
	11.16	Password: A mobile device and/or approved BYOD password policy has been put in place and enforced through technical controls to prohibit the changing of authentication and password lengths requirements.

	11.17	Policy: The BYOD policy clearly outlines requirements for the user to install anti-malware software, perform data backups, and not use unapproved application stores.
	11.18	Remote wipe: Technical controls have been put in place through a central mobile device management system to allow for remote company-provided data wipe off on all mobile devices and approved BYOD.
	11.19	Security patches: Technical controls have been put in place through a central mobile device management system to allow for remote software updates and patch validations on all mobile devices and approved BYOD.
	11.20	Users: The BYOD policy clearly outlines the servers and systems permitted for use or access by approved BYOD.
	12	**Do you consistently execute information protection processes and procedures?**
	12.1	Creation and maintenance of a baseline configuration of corporate IT and/or ICS systems incorporating security principles (e.g., concept of least functionality).
	12.2	Implementation of a system development life cycle (SDLC) process to manage systems.
	12.3	Configuration change control processes are in place.
	12.4	Conductance, maintenance, and testing of data backups.
	12.5	Assurance that policy and regulations regarding the physical operating environment for organisational assets are met.
	12.6	Destruction of data according to policy.
	12.7	Continuous improvement of protection processes.
	12.8	Effectiveness of protection technologies is shared.
	12.9	Development and management of response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery).
	12.10	Testing of response and recovery plans.
	12.11	Inclusion of cybersecurity in human resources practices (e.g., deprovisioning, personnel screening).
	12.12	Development and implementation of a vulnerability management plan.
	13	**Do you actively perform cryptography activities?**

	13.1	Entitlement: Encryption keys have identifiable owners (binding keys to identities) and there is an encryption key management policy in place.
	13.2	Key generation: Policies and procedures have been established for the management of cryptographic keys (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Where a cloud service provider is involved, the organisation ensures that upon request, the cloud service provider informs the organisation of any changes within the cryptosystem, especially if organisational data is used as part of the service, and/or the organisation has some shared responsibility over implementation of the control.
	13.3	Storage and access: Policies and procedures have been established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.
	14	**Do you keep a log of all your assets' maintenance and repairs?**
	14.1	Maintenance and repair of organisational assets are performed and logged with approved and controlled tools.
	14.2	Remote maintenance of organisational assets is approved, logged, and performed in a manner that prevents unauthorised access.
	15	**Do you actively manage all your cybersecurity protective technologies according to established policy, processes and procedures?**
	15.1	Determination, documentation, implementation, and review of audit/log records in accordance with policy.

	15.2	Protection and usage restriction of removable media according to policy.
	15.3	Incorporation of the principle of least functionality by configuring systems to provide only essential capabilities.
	15.4	Protection of communications and control networks.
	15.5	Implementation of mechanisms (e.g., failsafe, load balancing, hot swap) to achieve resilience requirements under normal and adverse situations.
	16	**Do you perform data security assurance?**
	16.1	Audit planning: Development and maintenance of cybersecurity audit plans to address business process disruptions.
	16.2	Independent audits: Independent cybersecurity reviews and assessments are performed at least annually to ensure that the organisation addresses nonconformities of established policies, standards, procedures, and compliance obligations.
	16.3	Regulatory compliance: The organisation has created and maintains a control framework which captures standards, regulatory, legal, and statutory requirements relevant for business needs. The control framework is reviewed at least annually to ensure changes that could affect the business processes are reflected.
	17	**Do you regularly conduct cybersecurity awareness and training?**
	17.1	Awareness training and information for all users.
	17.2	Privileged users understand their roles and responsibilities.
	17.3	Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.
	17.4	Senior executives understand their roles and responsibilities.
	17.5	Physical and cybersecurity personnel understand their roles and responsibilities.
DETECT	**18**	**Do you analyse cybersecurity anomalies and events?**
	18.1	Establishment and management of a baseline of network operations and expected data flows for users and systems.
	18.2	Analysis of detected events to understand attack targets and methods.

	18.3	Collection and corelation of event data from multiple sources and sensors.
	18.4	Determination of the impact of events.
	18.5	Establishment of incident alert thresholds.
	19	**Do you conduct cybersecurity research and development?**
	19.1	Conductance of cybersecurity research and development.
	20	**Do you perform continuous monitoring of cybersecurity incidents?**
	20.1	Monitoring of the network to detect potential cybersecurity events.
	20.2	Monitoring of the physical environment to detect potential cybersecurity events
	20.3	Monitoring of personnel activities to detect potential cybersecurity events
	20.4	Detection of malicious code.
	20.5	Detection of unauthorised mobile code.
	20.6	Monitoring of external service providers' activities to detect potential cybersecurity events.
	20.7	Monitoring for unauthorised personnel, connections, devices, and software.
	20.8	Conductance of vulnerability scans.
	21	**Do you have an established cyberthreats detection processes?**
	21.1	Definition of roles and responsibilities for detection to ensure accountability.
	21.2	Compliance of detection activities with all applicable requirements.
	21.3	Testing of detection processes.
	21.4	Communication of event detection information.
	21.5	Continuous improvement of detection processes.
RESPOND	**22**	**Do you have a cybersecurity response plan in the event of a cyberattack?**
	22.1	Execution of response plan during or after a cybersecurity incident.
	23	**Do you have a cybersecurity response communications plan in the event of a cyberattack?**

	23.1	Personnel know their roles and order of operations when a response is needed.
	23.2	Reporting of incidents consistent with established criteria.
	23.3	Information is shared consistent with response plans.
	23.4	Coordination with stakeholders occurs consistent with response plans.
	23.5	Voluntary sharing of information with external stakeholders to achieve broader cybersecurity situational awareness
	24	**Do you actively perform cyberthreats analysis resulting from the cyberthreats detection process?**
	24.1	Notifications from detection systems are investigated.
	24.2	Understanding of the impact of the incident.
	24.3	Conductance of forensics activities.
	24.4	Categorisation of incidents consistent with response plans.
	24.5	Establishment of processes to receive, analyse and respond to vulnerabilities disclosed to the organisation from internal and external sources (e.g. internal testing, security bulletins, or security researchers).
	25	**Do you have a cybersecurity mitigation strategy in the event of a cyberattack?**
	25.1	Containment of incidents.
	25.2	Mitigation of incidents.
	25.3	Mitigation and/or documentation of newly identified vulnerabilities as accepted risks.
	26	**Do you have a cybersecurity response improvement plan to capture lessons learned after a cyberattack?**
	26.1	Incorporation of response plans lessons learned.
	26.2	Updating of response strategies.
RECOVER	**27**	**Do you have a cybersecurity recovery plan after a cyberattack?**
	27.1	Execution of recovery plan during or after a cybersecurity incident.
	28	**Do you have a cybersecurity recovery improvement plan to capture lessons learned after a cyberattack?**
	28.1	Incorporation of recovery plans lessons learned.
	28.2	Updating of recovery strategies.

	29	**Do you have a cybersecurity recovery communications plan after a cyberattack?**
	29.1	Management of public relations.
	29.2	Repairment of reputation after a cybersecurity incident.
	29.3	Communication of recovery activities to internal and external stakeholders as well as executive and management teams.