CYBER GOVERNANCE IN THE WATER SECTOR

Volume 4 – Education and awareness guidelines

Report to the
WATER RESEARCH COMMISSION

by

Suné von Solms, Annlizé Marnewick, Masike Malatji and Wikus Erasmus
University of Johannesburg

WRC Report No. 3060/4/22
ISBN 978-0-6392-0366-9

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. 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 3: Water sector cybersecurity resilience strategy and assessment (WRC Report No. 3060/3/22)

DISCLAIMER

This report has been reviewed by the Water Research Commission (WRC) and approved for publication. Approval does not signify that the contents necessarily reflect the views and policies of the WRC, nor does mention of trade names or commercial products constitute endorsement or recommendation for use.

EXECUTIVE SUMMARY

South Africa appears to have fallen behind in securing and protecting cyberspace (Von Solms & Von Solms, 2015), where the prevalence of cybersecurity attacks and cybercrime has increased significantly, with state organisations having recently been targeted (South Africa Operational Risk Report, 2021). South Africa has been identified as one of the most targeted countries by cybercriminals (Lusthaus et al., 2020). Consequently, the country was ranked 1st out of 13 Southern African states and 73rd globally on financial crime and cybercrime. In addition, the critical infrastructure in South Africa remains highly vulnerable to cybercrime threats (South Africa Operational Risk Report, 2021).

Water management is performed by a range of organisations, from national departments to local municipalities. A wide range of corporate information technologies (IT) and operational technologies (OT) are deployed in the water and sanitation sector as utilities are increasingly using smart or connected industrial control systems. These connected technologies are vulnerable to cybersecurity threats. Various possible attacks have been identified, including sabotage or even damage by means of contamination injection, cyberattack or physical destruction.

The deployment of technology to protect security systems from cyberattacks is critical, but it has been shown in multiple instances that humans are the weakest link in the cybersecurity chain. Organisations continuously invest technological resources to reinforce their security dispositions, but regularly fall victim to unwanted intrusions to their information systems due to vulnerabilities caused by human activity on these systems. Human aspects of cybersecurity play a major role in the overall security of any sector. As one of the critical infrastructures, the water infrastructure must be protected from cyberattacks that might harm service delivery and the overall strategic objectives of the water service authorities. It is therefore important for the employees in the water sector to be cyber-aware.

This project focuses on determining the baseline awareness level of employees in the sector, developing a baseline cybersecurity skills framework for the sector, and developing training material based on the findings of the baseline awareness assessment.

RATIONALE

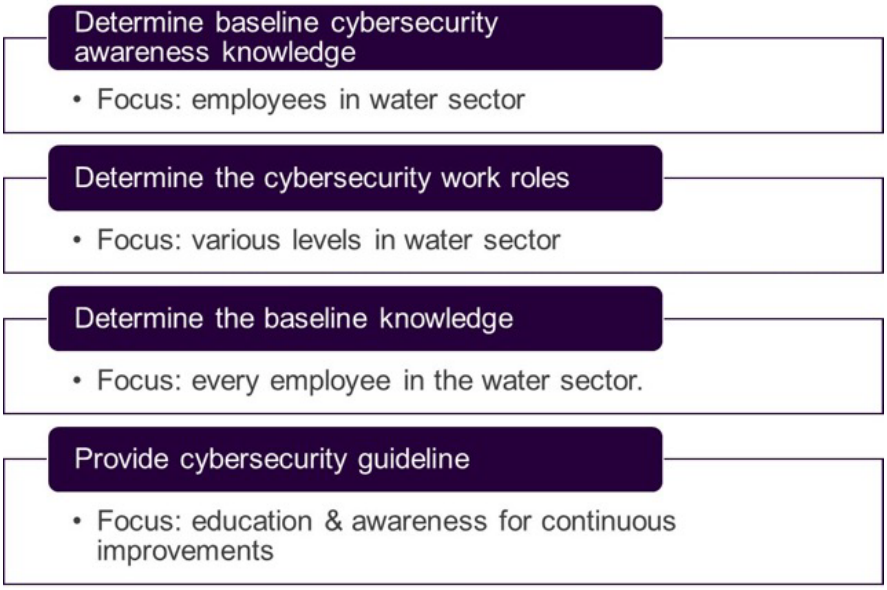
This work package includes multiple steps in measuring and identifying required cybersecurity awareness knowledge and work roles. Based on the findings of the work, two cybersecurity

training sets have been constructed. The first relates to the general cybersecurity awareness knowledge which every employee in the water sector should have. The second training set relates to professional qualifications which can be pursued by cybersecurity professionals in the water sector.

OBJECTIVES AND AIMS

The aim of the WP4 study was to determine the baseline cybersecurity awareness levels of the sector and to develop appropriate education and training material. The objectives of the study were as follows:

- Determine the baseline cybersecurity awareness level of the sector for all employees.
- Determine the cybersecurity work roles for the sector and the levels in the sector to which they apply.
- Determine the baseline knowledge which every employee in the sector should have.
- Provide guidelines for education and awareness continuous improvements.


Determine baseline cybersecurity awareness knowledge

- Focus: employees in water sector

Determine the cybersecurity work roles

- Focus: various levels in water sector

Determine the baseline knowledge

- Focus: every employee in the water sector.

Provide cybersecurity guideline

- Focus: education & awareness for continuous improvements

Figure 1: Focus areas

METHODOLOGY

The methodology followed in this project contains various steps, as summarised here:

Step 1: Determine the baseline cybersecurity awareness knowledge which all employees in the water sector should have.

Step 2: Derive a measuring tool to determine the baseline cybersecurity awareness knowledge of employees.

Step 3: Determine the baseline cybersecurity awareness knowledge of the employees in the water sector by applying the measurement tool developed in step 2.

Step 4: Based on the findings of steps 1 and 3, create cybersecurity training and education material which will address the general cybersecurity awareness requirements identified for employees in the water sector.

Step 5: Identify the work roles in the water sector and the level to which they apply. This will inform more specialised cybersecurity knowledge and skills which need to be included in the sector.

Step 6: Based on the work roles identified in step 5, present a set of professional training courses and certifications which can assist cybersecurity professionals in the water sector.

RESULTS AND DISCUSSION

The report includes results from three master's dissertations related to cybersecurity awareness and training in the water sector.

The first result is a framework identifying the minimum cybersecurity knowledge required of a typical employee in the water sector. Eight categories of cybersecurity risks are identified, as well as four mitigation methods that may be used to combat these risks. (R. Thomani, study titled: *Cybersecurity knowledge requirements for a water sector employee*, Supervisor: Prof AL Marnewick & co-supervisors: Prof S von Solms & Dr M Malatji)

The second result is a model developed to test cybersecurity awareness in the water sector. This model was utilised to test the general cybersecurity awareness level in the water sector and to develop training and education material for cybersecurity awareness. (S.B. Mufor, study titled: A measurement instrument to determine the level of cybersecurity awareness in the water sector, Supervisor: Prof AL Marnewick & co-supervisor: Prof S von Solms.)

The third result presents the work roles defined for cybersecurity practitioners which should be filled by the organisation to ensure that cyberthreats are prevented, mitigated, and detected to reduce this emerging risk. This work was utilised to create a set of professional training courses and certifications which can assist cybersecurity professionals in the water sector. (A. Melanie, study titled: The identification of cybersecurity work roles for the water sector in South Africa, Supervisor: Prof AL Marnewick & co-supervisors: Prof S von Solms & Dr M Malatji).

RECOMMENDATIONS

Cybersecurity education and awareness is critical for all organisations. An organisation might have strong technical cybersecurity controls in place, but it will not keep the organisation secure if its employees are not cyber secure. Therefore, it is of utmost importance to ensure that all employees, not just technical staff, have at least a basic working knowledge and understanding of cybersecurity principles. Technical staff in key positions requires advanced cybersecurity knowledge which can be obtained via professional certifications and courses.

Basic working knowledge and understanding of cybersecurity:

- Cybersecurity education and awareness should be a continuous process which must be informed by new knowledge as new approaches are used in new cybersecurity incidents.
- To determine the employees' level of cybersecurity awareness, a baseline must be created and then monitored to ensure improvement over time. The baseline can inform the organisation which specific elements need improvement and can then be targeted through organisation wide cybersecurity awareness sessions.
- There exists a wide range of online open-source training material available, which can be use by the organisation and individual employees to improve their cybersecurity awareness.
- Organisations must ensure that they integrate online training with interactive sessions to provide organizational context.
- Organisations should approach cybersecurity awareness training from three levels:
    - Individual: encourage self-learning to improve general cybersecurity awareness.
    - Organisation: conduct organisation-wide awareness sessions to address shortcomings in key areas as guided by the baseline cybersecurity awareness survey.
    - Executive / leadership: cybersecurity issues are not purely a technology problem and requires a layered approach to protect organisations, which includes training, strategy and knowledge regarding the correct reactions to cyber incidents.
- The improvement of cybersecurity awareness in a continuous process which requires regular cybersecurity awareness level measurements, training sessions and monitoring of new incidents and mitigation measures.

Advanced cybersecurity knowledge:

- Organisations must determine the key cybersecurity work roles required in their organisations.
- Organisations can utilise the guidelines presented in this document to develop career paths for technical personnel to obtain professional cybersecurity certifications.

- Professional cybersecurity training and education must be a continuous process which requires regular cybersecurity work role requirement assessments based on organisational needs and industry advancements.

It is acknowledged that organisational resilience can only be achieved through a layered approach with a combination of technical, formal, and informal mitigation strategies and that cybersecurity knowledge alone will not be sufficient. Aspects such as organisational and management support, policy, awareness and training, monitoring and auditing, employee involvement and communication, learning from experience, shared responsibility, continuous learning and empowerment of employees are required within an organisation to build organisational cyber resilience.

CONCLUSIONS

The report contains two cybersecurity training sets which can help entities in the water sector improve their general cybersecurity awareness knowledge and guide them on the professional qualifications which can be pursued by cybersecurity professionals in the water sector.

KNOWLEDGE DISSEMINATION

The research conducted under WP4 has led to an international peer-reviewed conference publication as well as three master's graduates. As a result, the content of this report is an outcome of the consolidation of the above research.

1. B. S. Mufor, A.L. Marnewick & S. von Solms, The development of cybersecurity awareness measurement model in the water sector, 17th International Conference on Cyber Warfare and Security (CCWS 2022), Vol. 17 No. 1 (2022), https://doi.org/10.34190/iccws.17.1.43

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

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AWWA	American Water Works Association
CSA	Cybersecurity awareness
CWF	Cybersecurity Workforce Framework
HAIS-Q	Human Aspects of Information Security Questionnaire
ICT	information and communication technologies
IPO	Input-process-output
IT	Information technology
NCPF	National Cybersecurity Policy Framework
NCSC	National Cyber Security Centre
NICE	National Initiative for Cybersecurity Education
NIST	National Institute for Standards and Technology
PICO	People, Intervention, Comparators, Outcome
SABS	South African Bureau of Standards
SCADA	Supervisory Control and Data Acquisition systems
SFIA	Skills Framework for the Information Age
WP	Work package

This page was intentionally left blank

1 INTRODUCTION AND OBJECTIVES

This body of work, also named Work Package 4 (WP4), focuses on the importance of cybersecurity awareness in the sector. This includes the following studies:

- The required awareness knowledge and skills of water sector employees
- How to determine the awareness baseline in the sector
- Determining the awareness baseline in the sector
- Determining the work roles in the water sector and the levels in the sector to which they apply

Based on the outcome of the above studies, cybersecurity awareness training material has been developed. The material was sourced from open-source cybersecurity training material made available by various cybersecurity organisations, academic organisations, governments, etc.

2 BASELINE CYBERSECURITY AWARENESS REQUIREMENTS

Globally, the water and wastewater sector was ranked number 4 in the global security incidents based on the Repository of Industrial Security Incidents (Panguluri et al., 2011). To date, systems that can protect themselves without involving the human element have not been realised, and as a consequence, systems are prone to be threatened by human action (both intentionally and unintentionally). Research shows that humans are the weakest link in cyberspace security. Therefore, there is a need to examine internal procedures and protection mechanisms to prevent cyberattacks related to the human aspects of these systems (Burghouwt et al., 2017). Building a cybersecurity culture has been argued by researchers to be essential in changing attitudes and perceptions as well as instilling good security behaviour in individuals (Alshaikh, 2020).

The creation of a cybersecurity culture within an organisation is not an easy task, but one of the fundamental aspects to create such a culture is that all employees must have a certain level of cybersecurity awareness (CSA). This section of work aims to determine what expertise employees are required to have to promote cybersecurity culture and awareness in the water sector. To determine the answer, a systematic literature review was conducted with the objective to develop approaches to build the cybersecurity knowledge and awareness of a typical employee and thus encourage a cybersecurity culture within organisations in the water sector. The focus of this research was on protecting the critical water infrastructure against sector-specific cybersecurity attacks.

2.1 Methodology to determine cybersecurity awareness requirements of employees

A systematic literature review was derived from Higgins and Green (2008), Xiao and Watson (2019) and Mohamed Shaffril (2020). The derived systematic literature review model followed in this research is illustrated and summarised in Figure 2: Systematic literature review process below.

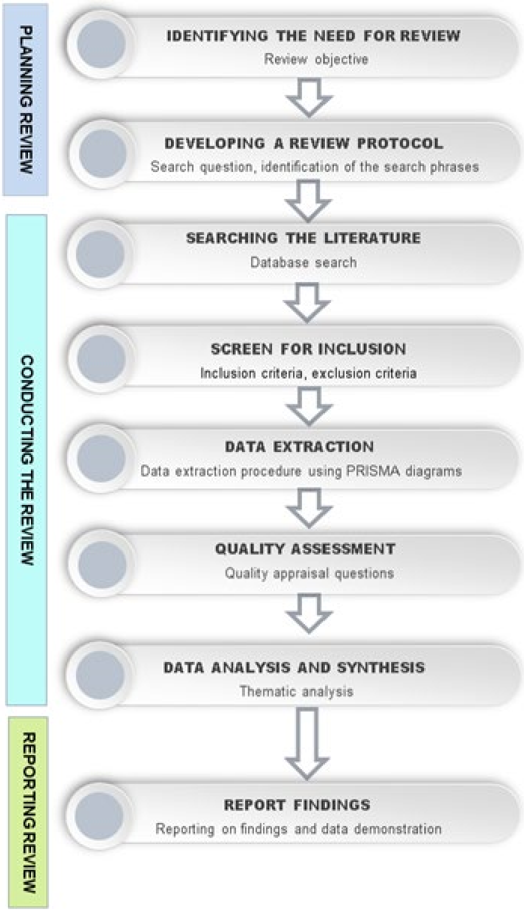

PLANNING REVIEW
IDENTIFYING THE NEED FOR REVIEW
Review objective
DEVELOPING A REVIEW PROTOCOL
Search question, identification of the search phrases
CONDUCTING THE REVIEW
SEARCHING THE LITERATURE
Database search
SCREEN FOR INCLUSION
Inclusion criteria, exclusion criteria
DATA EXTRACTION
Data extraction procedure using PRISMA diagrams
QUALITY ASSESSMENT
Quality appraisal questions
DATA ANALYSIS AND SYNTHESIS
Thematic analysis
REPORTING REVIEW
REPORT FINDINGS
Reporting on findings and data demonstration

Figure 2: Systematic literature review process

It can be seen that the process contains three main steps:

- **Planning the review**: This consists of two stages, the first being the identification of the need for a review, followed by the development of the review protocol.
- **Conducting the review**: This consists of five stages. The first stage will be the identification of research, followed by the selection of primary studies, study quality assessment, data extraction and data synthesis.
- **Reporting the review**: This entails reporting on the findings and data demonstration.

2.2 Planning the review

Identifying the need for a review

The objective of the systematic review was to determine what knowledge is essential for typical employees in the water sector to encourage a cybersecurity culture within the organisation. This systematic literature review was required in order to gather and summarise all the existing literature that presented evidence on existing and anticipated sector-specific CSA. This evidence assisted in determining the knowledge and capabilities required by an employee in the sector in order to curb cybersecurity-related attacks.

Developing a review protocol

The research question was framed so as to formulate a combination of keywords that could be used in the electronic databases. Below is a summary of the key search phrases and search strategy utilised.

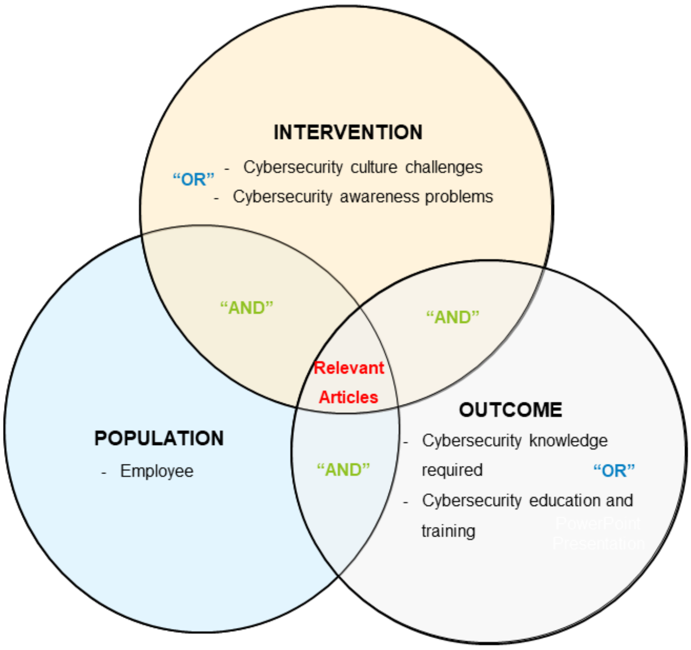

INTERVENTION
"OR"
- Cybersecurity culture challenges
- Cybersecurity awareness problems
"AND"
"AND"
Relevant Articles
POPULATION
- Employee
"AND"
OUTCOME
- Cybersecurity knowledge required
"OR"
- Cybersecurity education and training

Figure 3: Combining concepts for search sets

2.3 Conducting the review

Searching the literature

Databases in the domain of cybersecurity awareness and knowledge in the water sector include:

- ProQuest
- IEEE
- Emerald
- Engineering Village
- Wiley Online Library
- Science Direct

In addition, Google Scholar was used to source studies together with their corresponding databases.

Screening for inclusion and exclusion

Below is the model for the detailed inclusion/exclusion criteria.

Table 1: Inclusion criteria (Svahnberg et al., 2010)

STUDY INCLUSION CRITERIA	
Language in article	Articles delivered in English were used to avoid tampering with the output quality.
Article is peer-reviewed	To ensure the quality of the study, only peer-reviewed studies were used.
Article is in full text	Only full-text articles were included to accommodate comprehensive reading.
Type of article	The article could be comparative, action research, case study, survey, emphatic study.
Article relation	The article was related to cybersecurity knowledge and awareness in the water sector.
Article discussion	The article dealt with cybersecurity knowledge requirements for creating awareness.
Article evaluation and analysis	Existing cybersecurity knowledge of employees in the water sector was evaluated and analysed in the article.

Table 2: Exclusion criteria (Svahnberg et al., 2010)

STUDY EXCLUSION CRITERIA	
Articles not matching criteria	Articles that did not comply with the inclusion criteria were excluded.
Articles not in English	Articles not written in English were excluded; this may have affected the accuracy of the research.
Unverified articles	To avoid misleading information, articles that were not peer-reviewed were excluded.
Duplicated articles	DOI numbers were used to identify repeating articles from different databases.
Unreliable sources	Unreliable sources such as Wikipedia, Ask.com, Encarta.msn.com, Answers.com were not used.

Data extraction

To ensure a transparent and complete reporting of the systematic review and meta-analysis (Liberati et al., 2009), the following steps were taken:

- **Step 1: Identification of studies.** The databases were searched by applying search keys derived from the search strategy. A total of 2 013 documents were retrieved from the six databases.
- **Step 2: Screening for removing duplicates**. The total number of records identified was extracted after duplicates had been removed. A total of 633 duplicates were found and 1 380 distinctive document titles remained.
- **Step 3: Screening articles for inclusion based on abstract**. The inclusion and exclusion criteria were applied. The article abstracts were screened through coding that was undertaken by applying the 55 keyword codes to screen the abstract of the 1 380 distinctive documents to identify relevant documents. 1 215 documents were removed, and a total of 165 documents were selected for further reading in step 4.
- **Step 4: Screening articles for eligibility.** Full-text articles were screened for eligibility by applying the inclusion and exclusion criteria. A total of 134 documents were found to be irrelevant, and they were removed, leaving 30 documents. After further in-depth study, an additional 7 articles were removed as they were not applicable, leaving 23 studies.
- **Step 5: Included studies for qualitative synthesis**. A final total of 23 studies were analysed to identify the general CSA knowledge which all employees on the water sector must have.

The process followed is summarised in Figure 4 below:

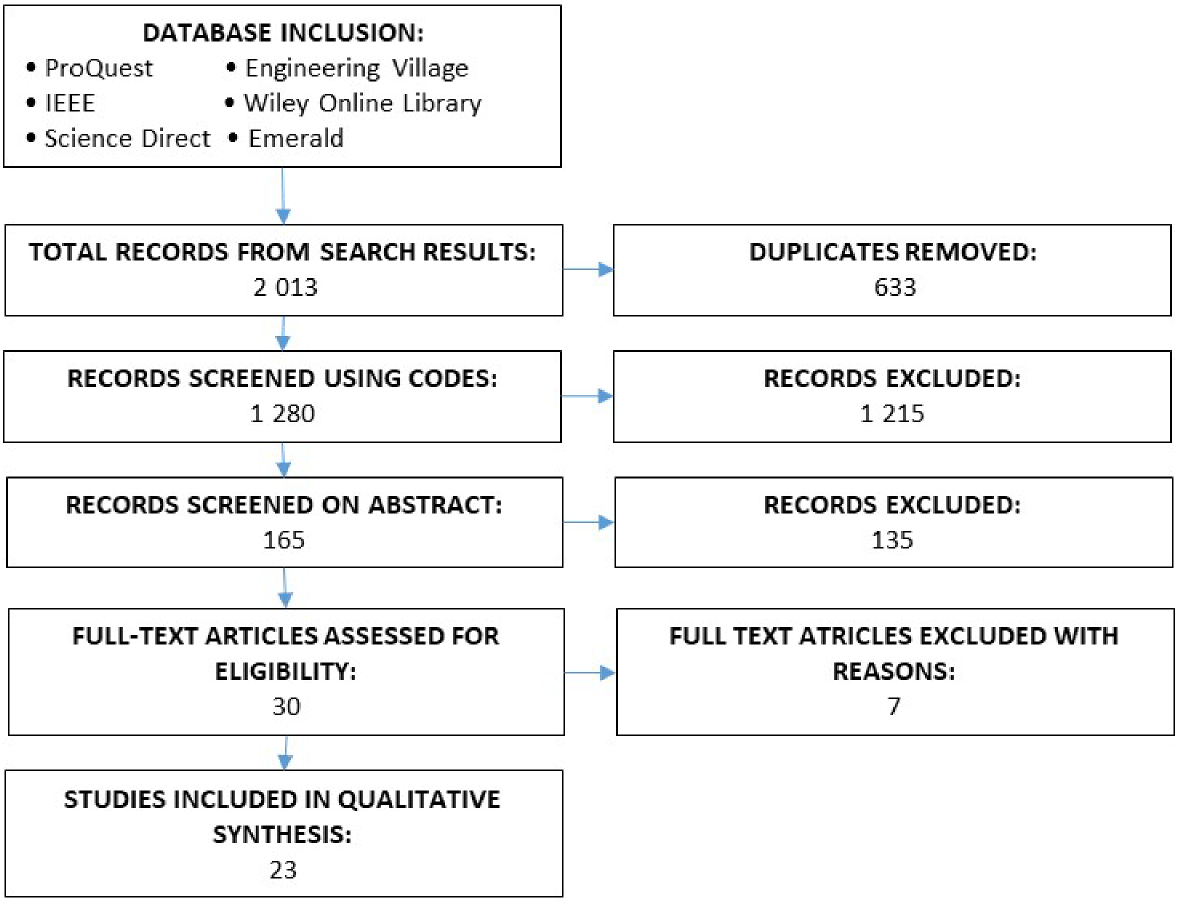

DATABASE INCLUSION:
• ProQuest
• IEEE
• Science Direct
• Engineering Village
• Wiley Online Library
• Emerald
TOTAL RECORDS FROM SEARCH RESULTS: 2 013
DUPLICATES REMOVED: 633
RECORDS SCREENED USING CODES: 1 280
RECORDS EXCLUDED: 1 215
RECORDS SCREENED ON ABSTRACT: 165
RECORDS EXCLUDED: 135
FULL-TEXT ARTICLES ASSESSED FOR ELIGIBILITY: 30
FULL TEXT ATRICLES EXCLUDED WITH REASONS: 7
STUDIES INCLUDED IN QUALITATIVE SYNTHESIS: 23

Figure 4: Data extraction process

Quality assessment

The remaining studies were subjected to a quality assessment to assist in investigating whether quality differences explained differences in the study results. An additional article was excluded through this process. The final articles are listed in Table 3 below:

Table 3: Selection of final articles

Study ID	Reference	Reason for inclusion
S1	Adams and Makramalla (2015)	The study focused on cybersecurity skills training.
S2	AlMindeel and Martins (2021)	The study dealt with employee information security awareness.
S3	Alshaikh (2020)	The study focused on developing a cybersecurity culture to influence employee behaviour.
S4	Carlton et al. (2019)	The study looked into mitigating cyberattacks through measuring cybersecurity skills.
S7	Chowdhury and Gkioulos (2021)	This study focused on cybersecurity training for protecting critical infrastructure.
S8	Ani et al. (2016)	This study focused on understanding the employee cybersecurity knowledge and skills capabilities for developing a skilled workforce.
S10	Erdogan et al. (2021)	The study focused on cybersecurity training using cyber-ranges.
S11	Ficco and Palmieri (2019)	This study focused on cybersecurity education and training programmes.
S12	Jin et al. (2018)	The study focused on game-based cybersecurity training.
S14	Karampidis et al. (2019)	The study focused on personnel training for identifying cybersecurity threats.

Study ID	Reference	Reason for inclusion
S15	Limba et al. (2019)	The study focused on providing theoretical aspects of the cybersecurity management model which can be used to ensure the security of critical infrastructure.
S18	Mishra et al. (2015)	The study focused on training in critical infrastructure protection.
S20	Nagarajan et al. (2012)	The study focused on CSA and cyberskills training.
S22	Dahlian Persadha et al. (2016)	The study's focus was on CSA.
S23	Prins et al. (2020)	The study focused on CSA levels and knowledge.
S24	Rege (2016)	The study focused on developing anticipatory cybersecurity measures.
S25	Khan et al. (2020)	The study focused on CSA and training.
S26	Rege et al. (2020)	The study focused on developing a social engineering awareness and training programme.
S27	Turkanović et al. (2019)	The focus of the study was on the cybersecurity education model from the information systems and information technology perspective.
S28	Varga et al. (2018)	The study's focus was on acquiring cybersituational awareness.
S29	Da Veiga (2016)	The study focused on the measure of a cybersecurity culture.
S30	Zhang et al. (2021)	The focus of the study was on cybersecurity and awareness training programmes.

Data analysis and synthesis

A thematic analysis was conducted on the selected articles. The five stages of Braun and Clarke (2006) are indicated below:

- Becoming familiar with the data
- Generating initial codes
- Searching for themes
- Reviewing the themes
- Reporting on themes

The summary of findings and data demonstration will be discussed further in the next section.

2.4 Results

The themes for identifying the cybersecurity challenges and the corresponding themes for building cybersecurity knowledge emerged through the use of codes. Codes with common features were allocated to the appropriate and relevant themes. The theme aimed to capture important details in the data through the research question to present patterned response or meaning in the data set (Braun & Clarke, 2006). Coding of text can be done in as many different themes as they fit (Nowell et al., 2017).

Themes for cybersecurity challenges

Eight themes were identified for cybersecurity challenges. These themes assisted in identifying the blocks of knowledge that general employees should have to protect the critical infrastructure. The themes below were developed based on the codes retrieved from the 23 studies.

The different types of cyberattacks were identified by analysing the 23 articles. The common types of cybersecurity threats indicated in each study were highlighted and allocated a single digit per study. Figure 5 below is the summary of different types of cyberattacks that are prevalent in critical infrastructure.

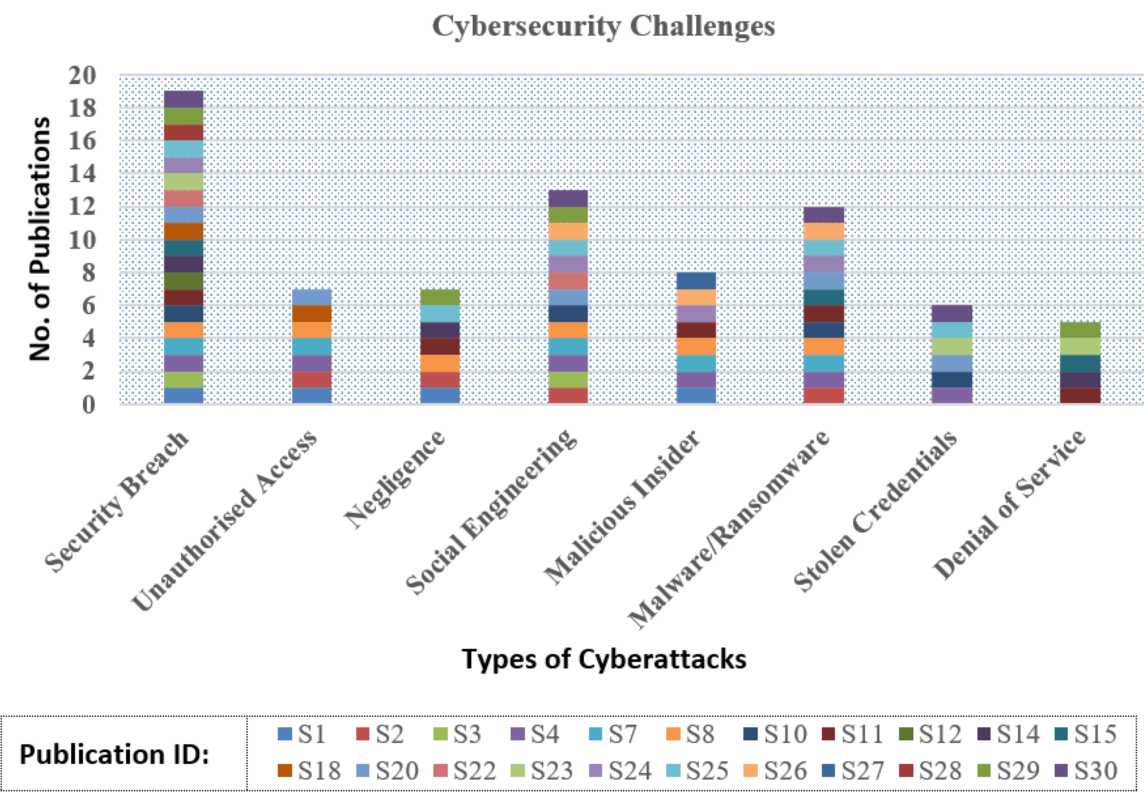


Figure 5: Types of cybersecurity threats per study

The frequency of the number of codes in each theme for methods of building cybersecurity knowledge is indicated in Table 4.

Table 4: Summary of themes for cybersecurity challenges and frequency of codes

Study ID	Themes for cybersecurity challenges	Code frequency	% articles
S1, S3, S4, S8, S10, S11, S14, S15, S18, S20, S22, S23, S24, S25, S28, S29, S30	Security breaches	18	24%
S1, S2, S7, S8, S18, S20	Unauthorised access	7	9%
S1, S2, S11, S14, S25, S29	Negligence	7	9%

Study ID	Themes for cybersecurity challenges	Code frequency	% articles
S2, S3, S4, S7, S8, S10, S20, S22, S24, S25, S26, S29, S30	Social engineering	13	17%
S1, S4, S7, S8, S11, S24, S26, S27	Malicious insider	8	11%
S2, S4, S7, S8, S10, S15, S20, S24, S25, S26, S30	Malware/ransomware	12	16%
S4, S10, S20, S23, S25, S30	Stolen credentials	6	8%
S11, S14, S15, S23, S29	Denial of service	5	7%

It can be seen that the main themes identified include security breaches, social engineering, malware/ransomware and malicious insiders.

Themes for methods of mitigating cybersecurity threats

Four themes were identified for mitigating the identified cyberthreats. These themes assisted in determining methods for mitigating cybersecurity threats as identified from the 23 collected studies on which the systematic literature review was conducted. The common methods of building cybersecurity knowledge were allocated a single digit per study. Figure 6 below is a summary of different types of methods that can be used to build the cybersecurity knowledge of employees.

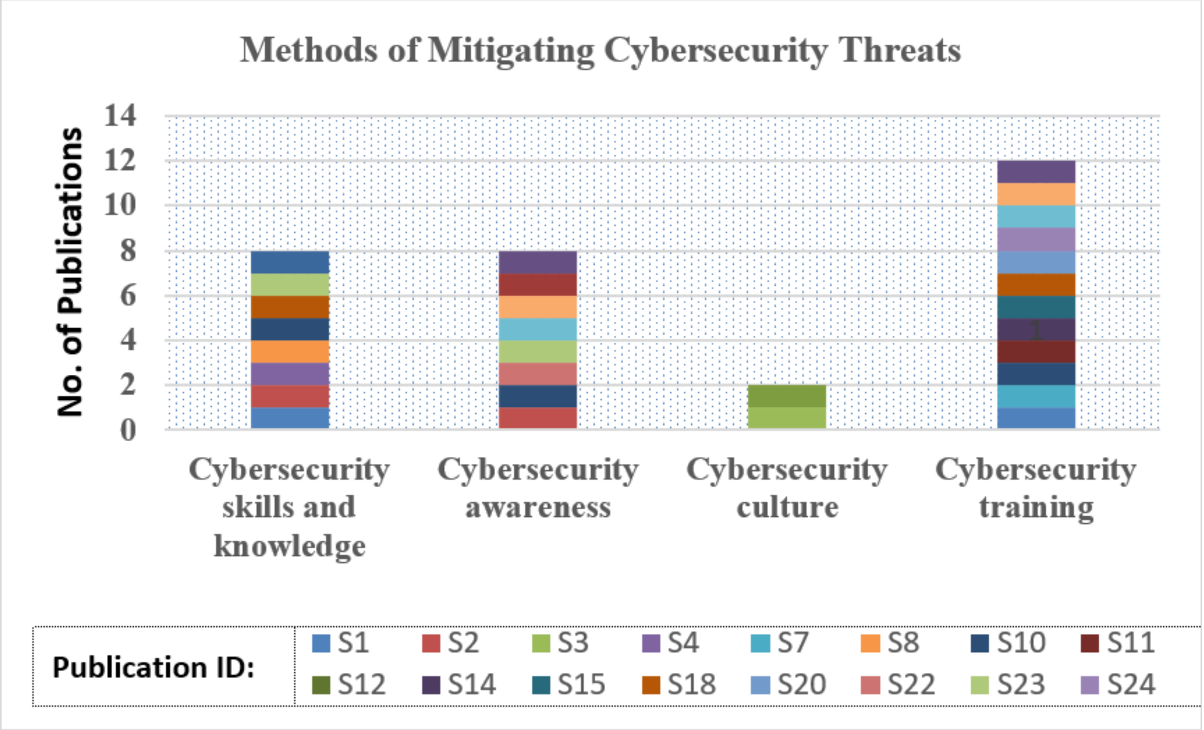


Figure 6: Methods of cybersecurity threat mitigation

The frequency of the number of codes in each theme for methods of building cybersecurity knowledge is indicated in Table 1 below.

Table 5: Summary of themes and frequency of codes

Study ID	Themes for methods of building cybersecurity knowledge	Code frequency	% articles
S1, S2, S4, S8, S10, S18, S23, S27	Cybersecurity skills and knowledge	8	27%
S2, S10, S22, S23, S25, S26, S28, S30	Cybersecurity awareness	8	27%
S3, S29	Cybersecurity culture	2	7%
S1, S7, S10, S11, S14, S15, S18, S20, S24, S25, S26, S30	Cybersecurity training	12	40%

It can be seen that training was the most commonly listed method for building cybersecurity knowledge in organisations.

Framework for defining cybersecurity knowledge

The basic input-process-output (IPO) model was followed in building the framework. The inputs considered included the eight cybersecurity challenges which were found most frequent as included in Table 4. The processes considered in the development of this framework were derived from the methods of building cybersecurity knowledge which were included in Table 5. As the aim of this framework is to determine the baseline cybersecurity knowledge of an employee in the water sector, the focus of the output is on the individual level (employee) as well as the organisational level (water sector).

By combining these three concepts and the information they contain, the IPO model for the framework was derived, as illustrated in Figure 7.

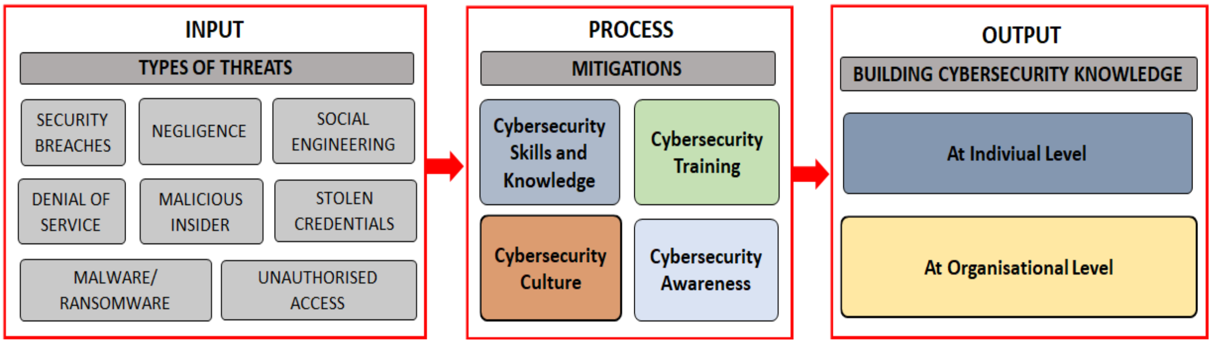
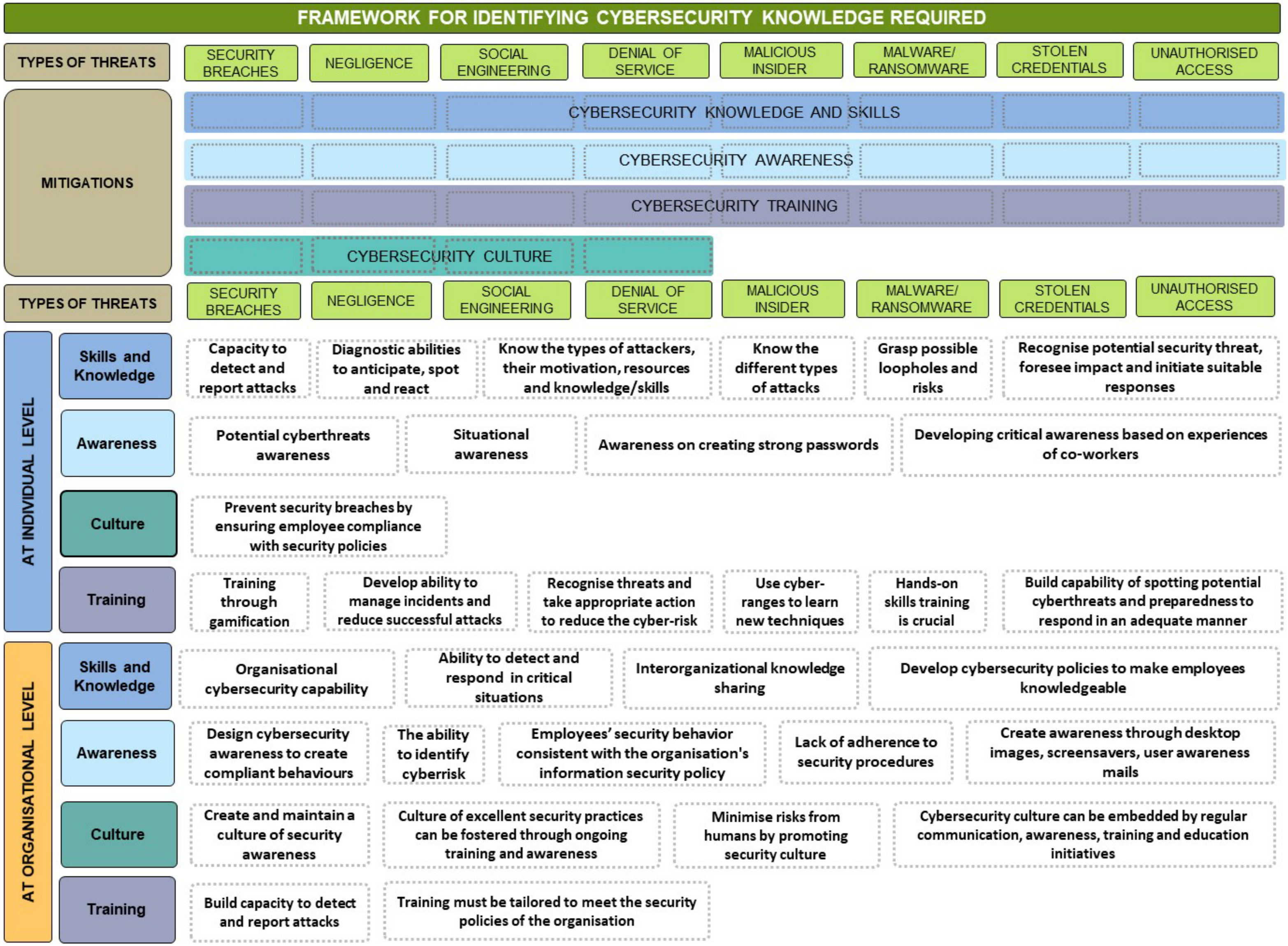


Figure 7: IPO model for building cybersecurity knowledge

The IPO model in Figure 7 is further expanded to form the comprehensive model. The procedure followed to derive the model in Figure 8 consists of the following steps:

- Types of threats: Eight common types of threats were identified from data synthesis and analysis as shown in Table 4.
- Mitigations: Four mitigations measures for reducing successful attacks were identified as shown in Table 5.
- Building knowledge at individual level: Minimal skills required by individuals to curb cyber risk were identified and summarised, with few examples listed. The skills are divided into the four mitigation methods identified.
- Building knowledge at organisational level: Minimal skills required at an organisational level to curb cyber risk were also identified, a few examples of measures required to reduce cyber risk were listed. The skills are divided into the four mitigation methods identified.

The final framework is depicted in Figure 8 below.



FRAMEWORK FOR IDENTIFYING CYBERSECURITY KNOWLEDGE REQUIRED

TYPES OF THREATS: SECURITY BREACHES; NEGLIGENCE; SOCIAL ENGINEERING; DENIAL OF SERVICE; MALICIOUS INSIDER; MALWARE/ RANSOMWARE; STOLEN CREDENTIALS; UNAUTHORISED ACCESS

MITIGATIONS:

- CYBERSECURITY KNOWLEDGE AND SKILLS
- CYBERSECURITY AWARENESS
- CYBERSECURITY TRAINING
- CYBERSECURITY CULTURE

TYPES OF THREATS: SECURITY BREACHES; NEGLIGENCE; SOCIAL ENGINEERING; DENIAL OF SERVICE; MALICIOUS INSIDER; MALWARE/ RANSOMWARE; STOLEN CREDENTIALS; UNAUTHORISED ACCESS

AT INDIVIDUAL LEVEL

Skills and Knowledge:

- Capacity to detect and report attacks
- Diagnostic abilities to anticipate, spot and react
- Know the types of attackers, their motivation, resources and knowledge/skills
- Know the different types of attacks
- Grasp possible loopholes and risks
- Recognise potential security threat, foresee impact and initiate suitable responses

Awareness:

- Potential cyberthreats awareness
- Situational awareness
- Awareness on creating strong passwords
- Developing critical awareness based on experiences of co-workers

Culture:

- Prevent security breaches by ensuring employee compliance with security policies

Training:

- Training through gamification
- Develop ability to manage incidents and reduce successful attacks
- Recognise threats and take appropriate action to reduce the cyber-risk
- Use cyber-ranges to learn new techniques
- Hands-on skills training is crucial
- Build capability of spotting potential cyberthreats and preparedness to respond in an adequate manner

AT ORGANISATIONAL LEVEL

Skills and Knowledge:

- Organisational cybersecurity capability
- Ability to detect and respond in critical situations
- Interorganizational knowledge sharing
- Develop cybersecurity policies to make employees knowledgeable

Awareness:

- Design cybersecurity awareness to create compliant behaviours
- The ability to identify cyberrisk
- Employees' security behavior consistent with the organisation's information security policy
- Lack of adherence to security procedures
- Create awareness through desktop images, screensavers, user awareness mails

Culture:

- Create and maintain a culture of security awareness
- Culture of excellent security practices can be fostered through ongoing training and awareness
- Minimise risks from humans by promoting security culture
- Cybersecurity culture can be embedded by regular communication, awareness, training and education initiatives

Training:

- Build capacity to detect and report attacks
- Training must be tailored to meet the security policies of the organisation

Figure 8: Cybersecurity knowledge framework

]

Minimal knowledge of employees

A general employee in the water sector should be knowledgeable on at least the eight types of cybersecurity threats identified in the study above:

- Security breaches
- Employee negligence
- Social engineering
- Denial of service
- Malicious insider
- Malware/ransomware
- Stolen credentials
- Unauthorised access

Mitigation measures

The protection of critical infrastructure can be achieved by building the knowledge of employees and increasing their CSA levels. This will enable them to detect, report and correctly react to cyberattacks. It is important for employees to be knowledgeable on the different types of cyberattacks, motivation, resources and skills of the attacker and understand possible loopholes and risks within the organisation. The other key element in the cybersecurity knowledge and skills bracket is the ability to recognise potential security threats, foreseeing the impact and initiating suitable responses. In an organisational setting, the cybersecurity knowledge and skills involve joint organisational cybersecurity capability of the staff, which includes the ability to detect and respond in critical situations, sharing of knowledge among employees and the development of policies aimed at making employees knowledgeable.

The second mitigation measure that leads towards building cybersecurity knowledge is cybersecurity training. At an individual level, employees can gain valuable skills through developing abilities to manage incidents and reduce successful attacks. Through training, individuals can develop abilities to recognise threats and take appropriate action. The capability of spotting cyberthreats and the preparedness to respond in an adequate manner can be achieved through different training methods with the more hands-on skills training deemed crucial. Hands-on skills training includes methods such as gamification and cyber-ranges. At an organisational level, cybersecurity training entails building the team’s capacity to detect and respond to attacks and the training must be such that it is tailored to meet the security policies of an organisation.

The third element in building cybersecurity knowledge is cybersecurity culture. Cybersecurity culture should be embedded within organisations in order to prevent security breaches. This can be achieved by ensuring that a culture of CSA is created and maintained within the organisation, fostering excellent security practices through ongoing training and awareness. Regular communication is important to maintain the culture of safe practices; this can be achieved through several initiatives, including education and awareness.

The fourth element for building the cybersecurity knowledge of employees is cybersecurity awareness. At an individual level, employees can develop situational awareness that will enable them to be aware of potential cyberthreats. It is good practice to create awareness about strong passwords to avoid easy access to critical infrastructure systems. Employees can develop critical awareness based on experiences of co-workers. At an organisational level, organisations should design and develop CSA for compliant behaviour to enable the team to identify cyber-risks. The security behaviour of employees must be in line with the organisation’s security procedures. Ways to create employee awareness include the use of desktop images, screensavers and regularly feeding the users information on awareness through emails.

This chapter details how the literature was analysed and synthesised to build a framework for identifying the minimum cybersecurity knowledge required by a typical employee in the water sector. Eight categories of cybersecurity risks were identified, as well as four mitigation methods that may be used to combat these risks. An organisation's attitude towards cybersecurity is frequently reflected in the knowledge and skills of its personnel (Ani et al., 2016). Knowledge and skills can reduce human error caused by a lack of cybersecurity knowledge and awareness, which is one of the major causes of cyberincidents. CSA in a company is therefore important (Prins et al., 2020).

Cybersecurity skills and knowledge, together with cybersecurity training, may improve the overall culture and awareness at individual and organisational levels. The cybersecurity culture dimension necessitates the organisation and each individual to have a comprehensive grasp of all security measures that can be utilised within the organisation to improve cybersecurity. This includes managing employees and giving a clear description of the abilities that each organisation member must achieve (Limba et al., 2019).

3 DETERMINING CYBERSECURITY AWARENESS OF SECTOR EMPLOYEES

The aim of this chapter is to develop a measurement instrument to evaluate the level of CSA of general employees in the water sector in South Africa. CSA is an important aspect for organisations to evaluate in order to fortify cybersecurity protocols and configurations. This chapter includes the development of a comprehensive instrument to measure CSA in the water sector using psychological inclinations of employees assessed in previous studies. There is considerable synergy with regard to cybersystem usage across industries, and as a result, this study took a broad-based approach in configuring an instrument that can be used to adequately assess CSA. Having a reliable instrument to measure CSA helps mitigate the failed attempts at preparing employees for imminent cyberdisruptions by pinpointing areas where the training is needed before campaigns can be organised.

This chapter shows that the psychology of employees with respect to CSA is compartmentalised into three traits: knowledge, attitude and behaviour. These three traits are assessed under the following eight focus areas to check employee resilience to cybersecurity:

1. IS policy adherence
2. Password management
3. Email use
4. Internet use
5. Social media use
6. Mobile devices
7. Information handling
8. Incident reporting

Chapter 4 includes the details of the implementation of the measurement instrument to evaluate the level of CSA of general employees in the water sector in South Africa. This chapter includes the development of the model to test CSA in the water sector.

3.1 Cybersecurity considerations for water sector

The water sector is one of the main targets of cyberattacks (The White House, 2013). Traditional water systems generally operate on Supervisory Control and Data Acquisition (SCADA) systems, which monitor a variety of processes along the value creation chain, including raw water extraction and/or collection, transport of water, monitoring and control of the purification process, treated water distribution and control of pressure boost pumps (Luiijf, 2008.

SCADA systems have largely been dependent on customised operational technology—technology which requires in-person operation (Hassanzadeh et al., 2020). However, according to Hassanzadeh et al. (2020), the SCADA infrastructure increasingly overlaps operational technology with IT systems, essentially exposing them to remote tampering or cybertampering. SCADA systems that integrate IT into their operations tend to increase vulnerabilities in the system. However, due to the dispersed nature of water systems, employees have little choice but to access these systems remotely to perform operational tasks (Hassanzadeh et al., 2020), and if these individuals are compromised, the entire system becomes vulnerable to pending attack. Third-party personnel such as SCADA manufacturers, who are allowed to perform maintenance on SCADA systems and who are usually given full access to these systems, are another source of risk. Luiijf et al. (2011) indicate that managers in the water sector have raised this as an area of vulnerability. There are many incidents where a lack of CSA can leave critical infrastructure, including water, vulnerable to cyberattacks. In many of the cases, the areas of vulnerability are simple issues, such as password management, email use, internet use and incident reporting.

3.2 Methodology to develop the cybersecurity awareness measurement tool

The comprehensive measurement instrument to determine the CSA of employees in the water industry was developed in four phases. A systematic literature review was conducted on publications by experts in the field to assess the tools that they have developed in the past, and how these tools were applied to study CSA levels (phases 1 and 2). The data from the identified literature was extracted and assessed (phase 3). This information was utilised to develop a measurement model based on other CSA tools previously tested in industry (phase 4). The following steps were taken in the development of the CSA measurement tool:

- Phase 1: Wide scope search of literature, which included the initial search for publications from databases, application of exclusion criteria, screening by title and removal of duplicates and restricted content.
- Phase 2: Final literature content selection, which included validation of publications via abstract, full-text quality appraisal process and backward referencing to identify additional content.
- Phase 3: Comparison of measurement theories, which included the identification of model base theory, selection of focus areas and measurement traits, as well as the identification of organisation type and status considerations.
- Phase 4: CSA model design, which included the selection of base theory, focus areas and measurement traits. It also included the consideration of water-specific aspects and the final model development.

The execution of these phases will be discussed in detail in the following sections.

3.3 Search strategy and selection of relevant material

A comprehensive search strategy was employed to avoid a random and distorted search process and to assure the reader of the level of diligence applied to complete the work presented (Meades, 2015). Systematic literature reviews have strict requirements for the implementation of search strategies and the selection of relevant material (Snyder, 2019).

To identify academic material that was considered relevant to the research objective, targeted searches were conducted using key terms often applied in the field of cybersecurity. The key terms were identified using a variation of the PICO (People, Intervention, Comparators, Outcome) model (Purssell & McCrae, 2020). This variation entails exposure (E) in place of intervention and the removal of comparators - PEO. The question to be answered was: *What are the current instruments available to measure CSA in industry in general?* In accordance with the PEO model, the following answers were used to determine the search terms, and the final terms are shown in Table 6:

- **People** (representing the sample space under investigation): industry
- **Exposure** (representing the level of exposure of people): cybersecurity awareness
- **Outcome** (representing the outcome required): instrument to measure awareness levels

Table 6: Key search terms and synonyms

Population	Exposure	Outcome		
Industry	*Cybersecurity*	*Awareness*	*Measurement*	*Instrument*
Organisation Company Employee Worker Human factor	Information security	Education Culture	Assessment Evaluation	Model Mechanism Tool Framework Questionnaire Study

Searching the literature

For this study, six academic databases were explored to find all relevant publications that could assist in the development of a CSA measurement tool:

- Association for Computing Machinery Digital Library (ACMDL)
- Emerald
- IEEE Xplore
- ScienceDirect
- SpringerLink

- Taylor & Francis Online

Screening for inclusion and exclusion

The model for the detailed inclusion/exclusion criteria is given in Tables 7 and 8.

Table 7: Inclusion criteria (Svahnberg et al., 2010)

STUDY INCLUSION CRITERIA	
Language in article	Articles delivered in English were used to avoid tampering with the output quality.
Article is peer-reviewed	To ensure the quality of the study, only peer-reviewed studies were used.
Article is in full text	Only full-text articles were included to accommodate comprehensive reading.
Type of article	The article could be comparative, action research, case study, survey, emphatic study.
Article relation	The article was related to cybersecurity knowledge and awareness.
Publication date	Articles were published between 2011 and April 2021.

Table 8: Exclusion criteria (Svahnberg et al., 2010)

STUDY EXCLUSION CRITERIA	
Articles not matching criteria	Articles not focused on the measurement of CSA were excluded.
Articles not in English	Articles not written in English were excluded; this may have affected the accuracy of the research.
Unverified articles	To avoid misleading information, articles that were not peer-reviewed were excluded, as were magazine and newspaper articles.
Duplicated articles	DOI numbers were used to identify repeating articles from different databases.
Unreliable sources	Unreliable sources such as Wikipedia, Ask.com, Encarta.msn.com, Answers.com were not used.

Data extraction

To ensure a transparent and complete reporting of the systematic review and meta-analysis (Liberati et al., 2009), the following steps were taken:

- **Step 1: Identification of studies.** The databases were searched by applying search keys derived from the search strategy. A total of 24 596 documents were retrieved from the 6 databases.
- **Step 2: Screening for removing duplicates and articles based on exclusion criteria**. The total number of records identified was extracted after duplicates had been removed as well as papers not meeting the above exclusion criteria. A total of 5 928 distinctive document titles remained.

- **Step 3: Screening articles for inclusion based on title**. These papers were screened via titles, removing any papers which did not focus on CSA. After the removal of duplicates and papers which could not be accessed, a total of 120 papers were retained for full content selection.
- **Step 4: Screening articles for inclusion based on abstract**. The retained publications were screened by abstract. All publications that did not specifically discuss the development of a measurement instrument for CSA in the abstract were excluded. A total of 25 papers were retained after the abstract validation step.
- **Step 5: Screening articles for eligibility and final inclusion for qualitative synthesis.** For the full-text analysis, the following research analysis question was asked: Did the author develop an instrument to measure CSA levels? This quality appraisal was used to determine the degree to which the selected studies met the criteria of the current study—the degree to which the studies answered each predefined research analysis question was scored on a 5-point scale, ranging from irrelevant (1) to inch-perfect (5). A further 7 publications were excluded, leaving a total of 18 publications. Backward referencing was utilised to identify relevant content. Four articles were referenced in most of the studies analysed, and these articles were included in the current research, bringing the total number of papers to 22.

The process followed is summarised in Figure 9 below:

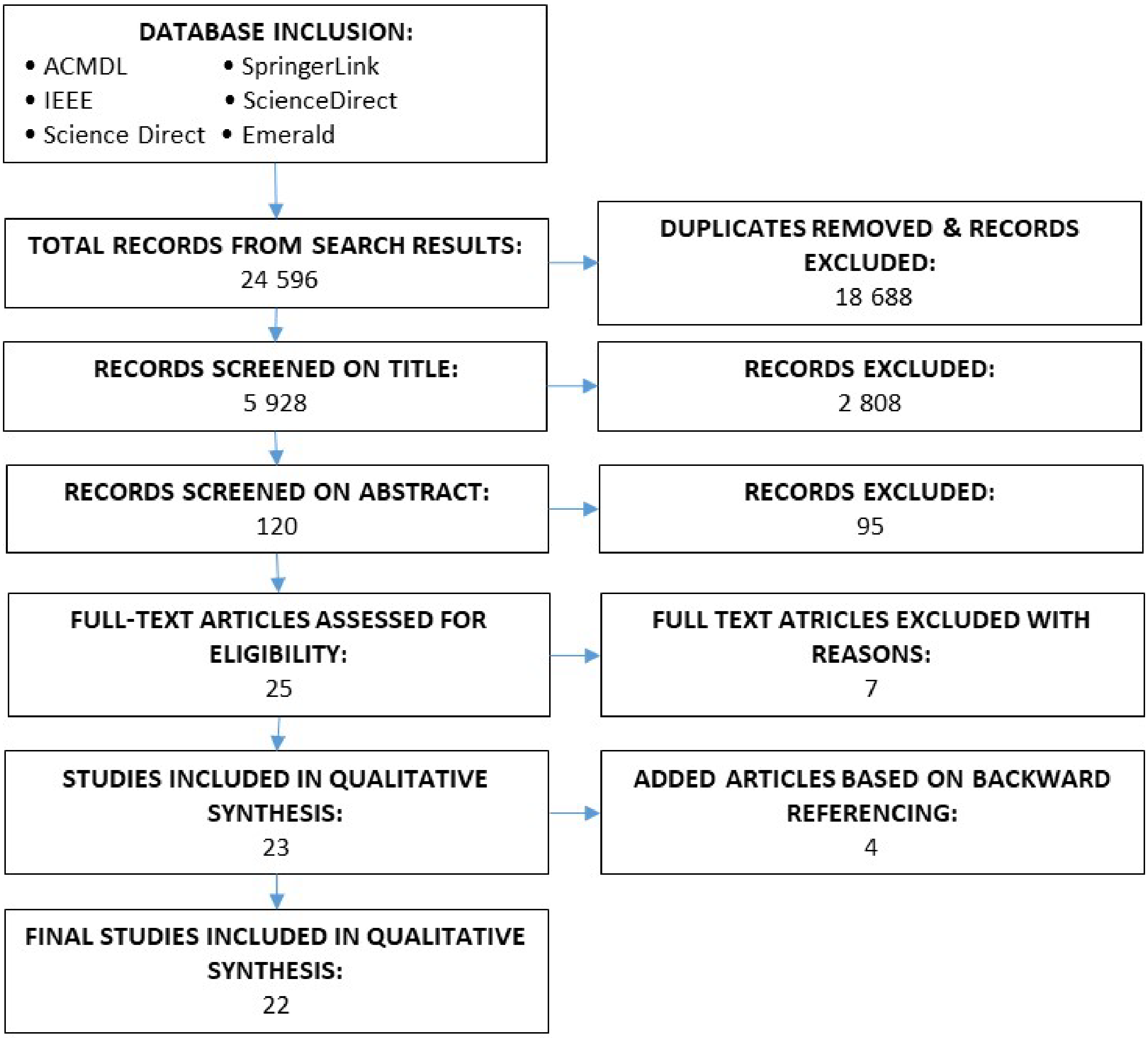

DATABASE INCLUSION:
• ACMDL
• IEEE
• Science Direct
• SpringerLink
• ScienceDirect
• Emerald
TOTAL RECORDS FROM SEARCH RESULTS: 24 596
DUPLICATES REMOVED & RECORDS EXCLUDED: 18 688
RECORDS SCREENED ON TITLE: 5 928
RECORDS EXCLUDED: 2 808
RECORDS SCREENED ON ABSTRACT: 120
RECORDS EXCLUDED: 95
FULL-TEXT ARTICLES ASSESSED FOR ELIGIBILITY: 25
FULL TEXT ATRICLES EXCLUDED WITH REASONS: 7
STUDIES INCLUDED IN QUALITATIVE SYNTHESIS: 23
ADDED ARTICLES BASED ON BACKWARD REFERENCING: 4
FINAL STUDIES INCLUDED IN QUALITATIVE SYNTHESIS: 22

Figure 9: Process for data collection

Quality assessment

The final list of articles retained for further analysis to develop the measurement tool for CSA is shown in

Table 9.

Table 9: List of publications for CSA model development

No.	Publication	Reference
1	Improving security awareness in the government sector	Amjad et al. (2016)
2	Securing our digital natives: A study of commonly experience [sic] internet safety issues and a one-stop solution	Agarwal and Singhal (2017)
3	Cybersecurity workforce in railway: Its maturity and awareness	Kour and Karim (2020)
4	Information security awareness and behavior: A theory-based literature review	Lebek et al. (2014)
5	Measurement of employee information security awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q): Case study at PT. PQS	Zulfia et al. (2019)
6	Measuring the information security awareness level of government employees through phishing assessment	Ikhsan and Ramli (2019)
7	Measurement of employee information security awareness: Case study at a government institution	Puspitaningrum et al. (2018)
8	A quick cybersecurity wellness evaluation framework for critical organizations	Jazri and Jat (2017)
9	Measuring information security awareness on employee [sic] using HAIS-Q: Case study at XYZ Firm	Cindana and Ruldeviyani (2019)
10	Measurement of employee information security awareness using analytic hierarchy process (AHP): A case study of foreign affairs ministry	Normandia et al. (2019)
11	A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument	Da Veiga (2016)
12	Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)	Parsons, McCormac, Butavicius et al. (2014)
13	The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies	Parsons et al. (2017)
14	Evaluating cybersecurity attitudes and behaviors in Portuguese healthcare institutions	Nunes et al. (2021)
15	Information security behavior: Development of a measurement instrument based on the self-determination theory	Gangire et al. (2020)
16	Semi-automated information security risk assessment framework for analyzing enterprises security maturity level	Abazi and Kő (2019)
17	Cyber security awareness, knowledge and behavior: A comparative study	Zwilling et al. (2020)
18	A model of information security awareness for assessing information security risk for emerging technologies	Mejias and Balthazard (2014)
19	A prototype for assessing information security awareness	Kruger and Kearney (2006)
20	A study of information security awareness in Australian government organisations	Parsons, McCormac, Pattinson et al. (2014)
21	Analysis of personal information security behaviour	Öƚütçü et al. (2016)
22	Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours	Hadlington (2017)

3.4 Development of CSA measurement instrument

This section details the analysis of the articles selected to construct an inclusive CSA measurement tool for the assessment of CSA levels in organisations of interest. Existing models were analysed for similarities, differences, advantages and disadvantages, and a coherent model is proposed based on the analysis.

Cybersecurity skills and knowledge, together with cybersecurity training, may improve the overall culture and awareness at individual and organisational levels.

Comparison of measurement theories

In phase 3, the selected articles were analysed to identify which base theory was utilised to measure the CSA of the employees in the study. Table 10 summarises the top base theories used in the selected studies.

Table 10: Summary of recurrence of base theory

No.	Base theory	Utilised in selected articles
1	Knowledge, Attitude, Behaviour (KAB) Model	10
2	Human Aspect of Information Security-Questionnaire (HAIS-Q)	8
3	Risky cybersecurity behaviour scale (RScB)	2
4	Attitude Towards Cybersecurity and Cybercrime in Business (ATC-IB)	2
5	ISO 27001	2
6	General deterrence theory (GDT)	2

One of the most popular models on which ten of CSA measurement models in the retained literature were developed was borrowed from the field of social psychology (Kruger & Kearney, 2006). This model is called the Knowledge, Attitude, Behaviour (KAB) Model. Parsons, McCormac, Butavicius et al. (2014), Parsons, McCormac, Pattinson et al. (2014) and Parsons et al. (2017) developed the Human Aspect of Information Security-Questionnaire (HAIS-Q), which was based on the KAB Model of Kearney and Kruger (2006). The HAIS-Q model itself appeared in eight different studies. Other models that appeared in the publications included Risky cybersecurity behaviour scale (RScB), Attitude Towards Cybersecurity and Cybercrime in Business (ATC-IB), ISO 27001 and general deterrence theory (GDT). Each model had varying areas on which they focused with regard to measuring the CSA of employees. The focus areas for each model were counted and the top recurring focus areas throughout the analysed studies were determined. Table 11 provides a summary of how many times each entry was measured in the selected publications.

Table 11: Summary of number of articles that measured this focus area

No.	Focus area	Number of times measured in selected articles
1	Internet use	15
2	Password management	14
3	Mobile devices	14
4	Email use	13
5	Social media use	13
6	Incident reporting	12
7	Information handling	10
8	IS policy adherence	6

The selected studies also focused on measuring certain traits possessed by the subjects for which CSA had to be assessed. The authors focused on different traits in order to determine the level of CSA for a given set of employees in each organisation evaluated. The most recurring traits were the knowledge, attitude and behaviour of the employees. The selected studies focused mainly on three types of institutions: public organisations, private organisations and academic institutions.

Cybersecurity awareness model design

Based on the comparison of the different models, the most popular method relied upon by the majority of the authors was the HAIS-Q model, which is based on the KAB Model developed by Kruger and Kearney (2006). They developed a measurement model pegged to three dimensions pertaining to human cognition: knowledge (what you know), attitude (what you think) and behaviour (what you do) (KAB), and each had varying importance levels according to the study. The KAB Model followed strict guidelines of sustainability, ease of use, use of scientific methods and compliance with the organisation of interest's unique requirement. The approach used by Parsons et al. (2017) in each publication was slightly improved with each iteration. Parsons, McCormac, Butavicius et al. (2014) outlined the development of HAIS-Q and its connection to the KAB Model in their 2014 publication after running a test trial with 500 Australian employees. The model identified seven focus areas: password management, email use, internet use, social networking sites, mobile computing, information handling and incident reporting – 2 as opposed to the six proposed by Kruger and Kearney (2006), with social media not being an area of interest at the time. The wide use of HAIS-Q, which has also been referenced in numerous publications geared towards measuring the CSA levels in a myriad of organisations, makes HAIS-Q a reliable model for further study. Puspitaningrum et al. (2018), Normandia et al. (2019), Cindana and Ruldeviyani (2019) and Zulfia et al. (2019) all based their measurement instruments on HAIS-Q. They assessed varying areas and types of organisations from government to private sector employees. The KAB Model and HAIS-Q were therefore selected based on popularity among other authors.

Focus area selection

The focus areas were selected by popularity, i.e. the number of times they were measured by previous authors. Table 12 shows which focus areas were common to the different studies and how the current study was developed based on the focus areas previously studied by the experts.

Table 12: Similarities of focus areas in KAB, HAIS-Q and current study

KAB Model	HAIS-Q	Current study
	Focus areas	
Adhere to policies	-	Adhere to policies
Action -› Consequences	-	-
Password management	Password management	Password management
Email use	Email use	Email use
Internet use	Internet use	Internet use
Mobile computing	Mobile computing	Mobile computing
Incident reporting	Incident reporting	Incident reporting
-	Information handling	Information handling
-	Social networking sites	Social networking sites

Key measurement trait selection

Similar to the selection of focus areas, the measurement traits were also selected based on popularity in previous academic publications by authors in the field of interest. The most popular measurement traits after the data extraction process were knowledge, attitude and behaviour.

The knowledge and attitude aspects of the questionnaire remained generally unaltered, following the traditional methodology of the HAIS-Q. For this section, respondents rated the items from 1-5 (1 = Strongly disagree and 5 = Strongly agree) However, items under the behavioural segment of the questionnaire followed the methodology applied in the RScB model, where respondents answered the questions based on retrospective behaviour in the six months preceding the evaluation. This was done because retrospective behaviour was considered more indicative of the respondent's level of awareness than simply having to agree or disagree with what the right behaviour should be in the different instances. The behavioural aspect of the HAIS-Q was modified to fit the RScB model and focus more on retrospective behaviour. The respondents used a scale of 1-5 (1 = Never and 5 = Daily or almost daily) for rating how often they engaged in a particular behaviour six months prior to the evaluation. The model covers all aspects discussed in the current study and could be used to assess the CSA levels of employees in the water sector by collecting data based on the response of each individual. A total of 22 questions in 8 focus areas formed the final measurement model, which is shown in Table 13.

Table 13: Final cybersecurity awareness measurement model

Sub-focus area	**Knowledge**	**Attitude**	**Behaviour**	**Behaviour (RScB modification)**
Focus Area: IS Policy Adherence				
Adhering to IS policy	It's acceptable to ignore IS protocol set out by management and IT department. *	No serious consequence can result from not following safety protocol at all times at work.	None	Ignores safety protocols because they are difficult or inconvenient to follow at all times.
Focus Area: Password Management				
Using the same password	It's acceptable to use my social media password on my work accounts. *	It's safe to use the same password for social media and work accounts. *	I use a different password for my social media and work accounts.	How often do you use your social media password on your work accounts?
Sharing passwords	I am allowed to share my work passwords with my colleagues. *	It's a bad idea to share my work password, even if a colleague asks for it.	I share my work password with colleagues. *	How often have you shared your work password with any of your colleagues in the specified period?
Using strong password	A mixture of letters, numbers and symbols is necessary for work passwords.	It's safe to have a work password with just letters. *	I use a combination of letters, numbers and symbols in my work passwords.	Used a password with a mixture of letters, numbers and symbols.
Focus Area: Email Use				
Clicking on links in emails from known senders	I am allowed to click on any links in the emails from people I know. *	It's always safe to click on links in emails from people I know. *	I don't always click on links in emails just because they come from someone I know.	Clicked on a link in an email that came from someone you know without appropriate verification.
Clicking on links in emails from unknown senders	I am not permitted to click on a link in an email from an unknown sender. *	Nothing bad can happen if I click on a link in an email from an unknown sender. *	If an email from an unknown sender looks interesting, I click on a link within it. *	Clicked on a link in an email from an unknown source because it looked interesting.
Opening attachments in emails from unknown senders	I am allowed to open an attachment from unknown senders. *	It's risky to open email attachments from an unknown sender.	I don't open email attachments if the sender is unknown to me.	Opened email attachment from an unknown sender.
Focus Area: Internet use				
Downloading files	I am allowed to download any files onto my work computer if they help me to do my work.	It can be risky to download files on my work computer.	I download any files onto my work computer that will help me get the job done. *	Downloaded files you considered necessary for work on your work computer.
Accessing dubious websites	While I am at work, I shouldn't access certain websites.	Just because I can access a website at work, it doesn't mean it's safe.	When accessing the internet at work, I visit any website that I want to. *	Visited random websites while at work.

Sub-focus area	Knowledge	Attitude	Behaviour	Behaviour (RScB modification)
Entering information online	I am allowed to enter any information on any website if it helps me do my job. *	If it helps me do my job, it doesn't matter what information I put on a website. *	I assess the safety of websites before entering information.	Assessed the safety of a website before entering information.
Focus Area: Social Media Use				
SM privacy settings	I must periodically review the privacy settings on my social media accounts.	It's a good idea to regularly review my social media privacy settings.	I don't regularly review my social media privacy settings. *	Reviewed your social media privacy settings.
Considering consequences	I can't be fired for something I post on social media. *	It doesn't matter if I post things on the social media that I wouldn't normally say in public. *	I don't post anything on social media before considering any negative consequences.	Considered the negative consequences of a social media post before uploading.
Posting about work	I can post what I want about work on social media. *	It's risky to post certain information about work on social media.	I post whatever I want about my work on social media. *	Posted about work on social media.
Focus Area: Mobile Device				
Physically securing mobile device	When working in a public place, I have to keep my laptop with me at all times.	When working in a café, it's safe to leave my laptop unattended for a minute. *	When working in a public place, I leave my laptop unattended.	Left your laptop unattended in a public place.
Sending sensitive information via Wi-Fi	I am allowed to send sensitive work files via a public Wi-Fi network. *	It's risky to send sensitive work files using a public Wi-Fi network.	I send sensitive work files using a public Wi-Fi network. *	Sent sensitive files using a public Wi-Fi network.
Shoulder surfing	When working on a sensitive document, I must ensure that strangers can't see my laptop screen.	It's risky to access sensitive work files on a laptop if strangers can see my screen.	I check that strangers can't see my laptop screen if I'm working on a sensitive document.	Checked over your shoulders to check if strangers are watching while you work on sensitive work material.
Focus Area: Information Handling				
Disposing of sensitive print-outs	Sensitive print-outs can be disposed of in the same way as non-sensitive ones. *	Disposing of sensitive print-outs by putting them in the rubbish bin is safe. *	When sensitive print-outs need to be disposed of, I ensure that they are shredded or destroyed.	Shredded or destroyed sensitive print-outs before disposing of them.
Inserting removable media	If I find a USB stick in a public place, I shouldn't plug it into my work computer.	If I find a USB stick in a public place, nothing bad can happen if I plug it into my work computer. *	I wouldn't plug a USB stick found in a public place into my work computer.	Plugged a USB stick found in a public area into your work computer.
Leaving sensitive material	I am allowed to leave print-outs containing sensitive information on my desk overnight. *	It's risky to leave print-outs that contain sensitive information on my desk overnight.	I leave print-outs that contain sensitive information on my desk when I'm not there. *	Left print-outs containing sensitive information on your desk in your absence.

Sub-focus area	Knowledge	Attitude	Behaviour	Behaviour (RScB modification)
Focus Area: Incident Reporting				
Reporting suspicious behaviour	If I see someone acting suspiciously in my workplace, I should report it.	If I ignore someone acting suspiciously in my workplace, nothing bad can happen. *	If I saw someone acting suspiciously in my workplace, I would do something about it.	Intervened after noticing someone acting suspiciously at your workplace.
Ignoring poor security behaviour by colleagues	I must not ignore poor security behaviour by my colleagues.	Nothing bad can happen if I ignore poor security behaviour by a colleague. *	If I noticed my colleague ignoring security rules, I wouldn't take any action. *	Taken action against a colleague who ignored security protocols.
Reporting all incidents	Its optional to report security incidents. *	It's risky to ignore security incidents, even if I think they're not significant.	If I noticed a security rules incident, I would report it.	Reported a security incident you noticed at work.

This chapter documents the process of the development of a model to test cybersecurity awareness in the water sector. This study was based on generic measurement instruments which were not specific to the water sector (although an effort was made to draw parallels between both test cases).

Considering how important CSA is in the water industry, a reliable CSA measurement tool can greatly assist in determining the level of CSA of employees in the sector and assist in the improvement of the security of the systems in this sector. The next chapter documents the process of evaluating the level of CSA of employees in the water sector, as employees can prove to be the point of entry for some of the most disastrous attacks, as demonstrated by Hassanzadeh et al. (2020). Chapter 5 builds on this work where, based on the baseline knowledge of CSA of employees, training programmes focusing on all areas of weakness are recommended for the improvement of the general level of CSA among employees and management.

4 CYBERSECURITY AWARENESS BASELINE STUDY

The aim of the survey was to assess the cybersecurity awareness of South Africa's water and sanitation sector. This chapter will include the results of the CSA baseline study. The aim of this CSA measurement is to investigate the cybersecurity knowledge, attitude and behaviour of employees of the sector in order to gain a better understanding of the level of awareness in the sector, which will help the country, water and sanitation sector, organisations and individual colleagues to fight cybercrime and stay resilient.

4.1 Data collection instrument

The description of the CSA measurement instrument was documented in Chapter 3. As discussed, the content of the measurement tool was based on the content of the Human Aspects of Information Security Questionnaire (HAIS-Q) with minor changes, including a change of tense and the addition of one focus area. However, when the measurement tool was to be utilised, it was decided to run the standard HAIS-Q used to derive a baseline of employees' CSA (Parsons et al., 2017) and not the altered measurement tool so that the results obtained could be compared with existing HAIS-Q results.

The HAIS-Q enables employees to identify strengths and weaknesses where more education and training are required to improve CSA (Parsons et al., 2017). This pre-tested questionnaire has been utilised in various organisations, sectors and countries (Parsons et al., 2017, Parsons et al., 2014). By using the existing questionnaire, results from other countries that have been published could be used as a cross-comparison (Parsons et al., 2014). The aim of this questionnaire is to examine the relationships between knowledge of policy and procedures, attitude towards policy and procedures and behaviour when using a work computer. The outline of the HAIS-Q is given in Figure 10 below.

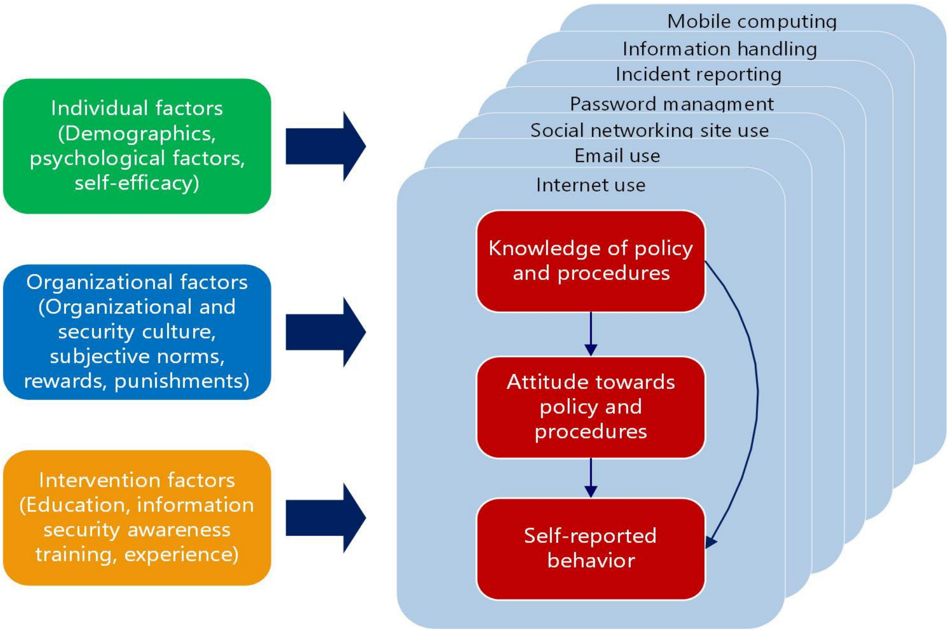

Individual factors (Demographics, psychological factors, self-efficacy)
Organizational factors (Organizational and security culture, subjective norms, rewards, punishments)
Intervention factors (Education, information security awareness training, experience)
Mobile computing
Information handling
Incident reporting
Password managment
Social networking site use
Email use
Internet use
Knowledge of policy and procedures
Attitude towards policy and procedures
Self-reported behavior

Figure 10: Human Aspects of Information Security (HAIS) model (Parsons et al., 2014)

4.2 Sample population

Real-world data was required from as many employees as possible in the water and sanitation sector. As these employees are not a defined population and belong to many organisations, the target population can be seen as hard to reach. In this type of population, snowball sampling is suggested to access the hidden population (Baltar & Brunet, 2012). This sampling approach utilises trust relationships to establish initial contact, and then uses these contacts to establish a chain of new contacts (Bryman & Bell, 2011).

Five separate approaches were followed to target employees from the water and sanitation sector through referral chains of snowball sampling:

1. The water research organisation distributed the survey to all their stakeholders in the water sector.
2. Relationships existed between the research team and three water boards, each in different provinces (Gauteng, KwaZulu-Natal and North West). The contact persons at these water boards distributed the survey to their employees and their personal network within the water sector.
3. Two municipalities based in Gauteng and Mpumalanga collaborated with the research project and distributed the survey to their employees.
4. The research project peer review group members were requested to distribute the survey to their personal network within the water sector.
5. A list of individual water practitioners known to the researchers were contacted and requested to distribute the questionnaire to their network of water sector employees.

4.3 Response rate

A total of 53 responses were received but only 39 responses could be used due to the incompleteness of the other 14 responses. The entire water sector employee base is difficult to estimate. The annual report of the Department of Water and Sanitation notes that the department has an employee base of more than 3 000 employees. This indicates a very low response rate if just the department employee base is used as an estimate (1,3%). As per the literature, online surveys do have low response rates, especially in unknown populations where the email addresses of the target population are not known and individual follow-up is not possible (Fricker & Schonlau, 2002).

4.4 Respondent profile

The questionnaire consisted of four sections. The first section focused on the questions relating to the respondents' employment status and typical computer usage. The majority of the respondents worked for a water board (31%), a municipal water service authority (20%) or a water research and development entity (18%). Figure 11 provides details about the type of organisation that the respondents worked for. Although the response rate was very low, the respondents were a diverse set across the sector.

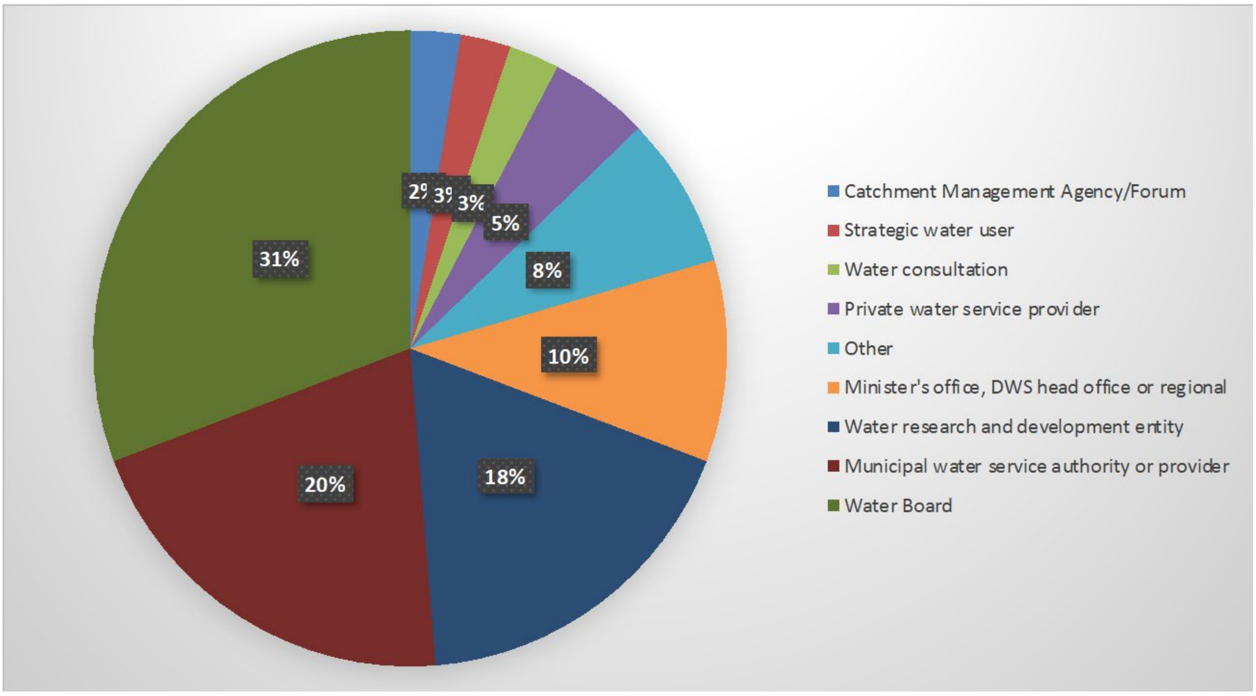


Figure 11: Type of organisation

As per the respondents' main job description, the majority (39%) were professionals, followed by technical support (21%) and executive and management (21%). Refer to Figure 12 for more details. The respondents also confirmed their employment status and 97% indicated that they were full-time employed compared to only 3% that were employed part time.

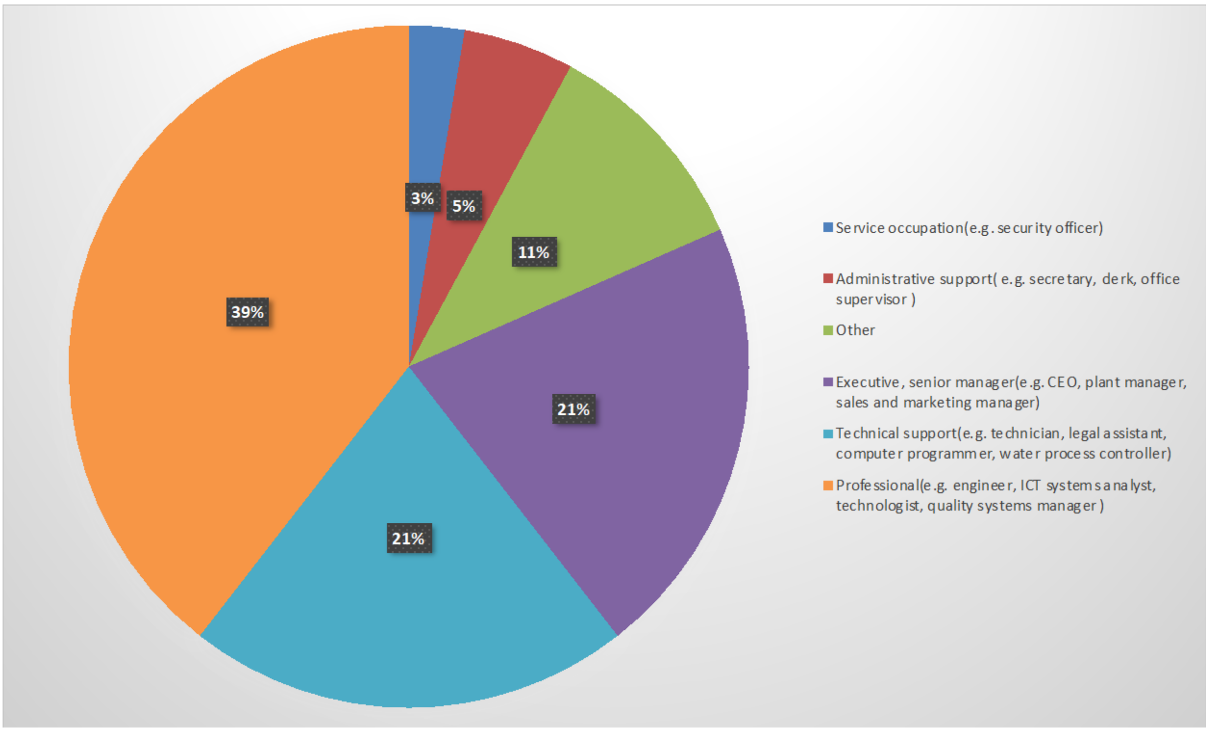


Figure 12: Job description

Most of the respondents (85%) were aware of their company's information security policy. There was a small percentage (5%) who were totally oblivious of any information security policy. This is concerning given the fact that 95% of the respondents worked more than 50% (i.e. 4 hours a day) a day on their computers or devices as per Figure 13.

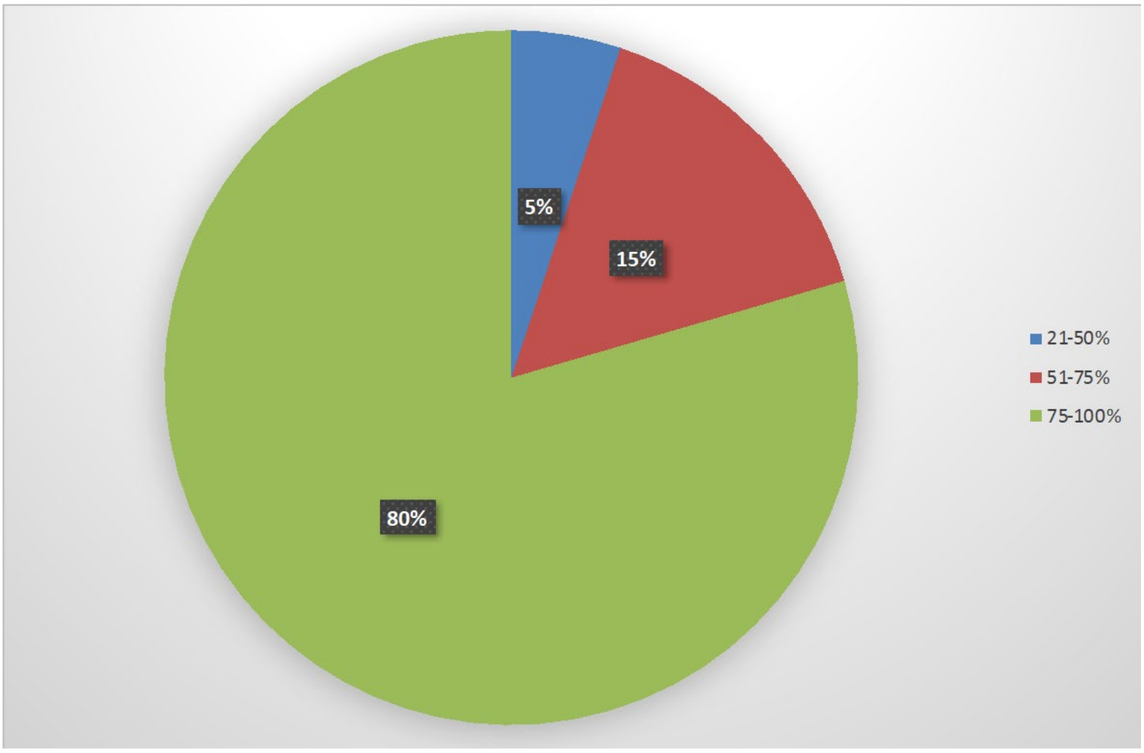


Figure 13: Time spent working on computer

4.5 Knowledge, attitude and behaviour

The first set of questions, section 2 of the questionnaire, focused on the knowledge respondents had of how they should use a computer for work. Section 3 focused on what the respondents thought about the computer use guidelines and lastly, section 4 focused on the actual behaviour of the respondents when using a computer for work (Parsons et al., 2017). There are seven focus areas in the HAIS-Q to understand how employees use a computer for work, namely password management, email use, internet use, social media use, mobile devices, information handling and incident reporting. The results of each of these focus areas are discussed in the next sections.

The next sections contain graphs where the mean value (maximum of 5) for every questionnaire question was calculated as well as the upper and lower deviations to understand the distribution of responses. It must be noted that in some instances, the upper limit exceeded the maximum value of 5. This is a direct consequence of the size of the standard deviation as well as the mean. If the mean was high and the standard deviation was large, then the upper limit exceeded the maximum value of 5. As prescribed by the questionnaire developers, certain questions should use reverse scoring. This is required so that for all the questions in the questionnaire, a high score indicates a high level of CSA.

Password management

This section of the questionnaire tested the respondents' knowledge of the guidelines pertaining to password usage. The questions posed to the participants are noted in Table 14.

Table 14: Password management questions (Parsons et al., 2017)

Focus area: *Password management*	**Knowledge**	**Attitude**	**Behaviour**
Using same password	It's acceptable to use my social media password on my work accounts. *	It's safe to use the same password for social media and work accounts.*	I use a different password for my social media and work accounts.
Sharing passwords	I am allowed to share my work passwords with my colleagues. *	It's a bad idea to share my work password, even if a colleague asks for it.	I share my work passwords with colleagues. *
Using a strong password	A mixture of letters, numbers and symbols is necessary for work passwords.	It's safe to have a work password with just letters.*	I use a combination of letters, numbers and symbols in my work password.

*Reverse scoring was used

The first aspect relates to knowledge of password management as displayed in Figure 14. The respondents had a high knowledge (4.05) of using a strong password. This can be attributed to the fact that the IT department enforced strong passwords. The respondents did not have high levels of knowledge when it came to using the same password for various systems and applications as well as sharing passwords.

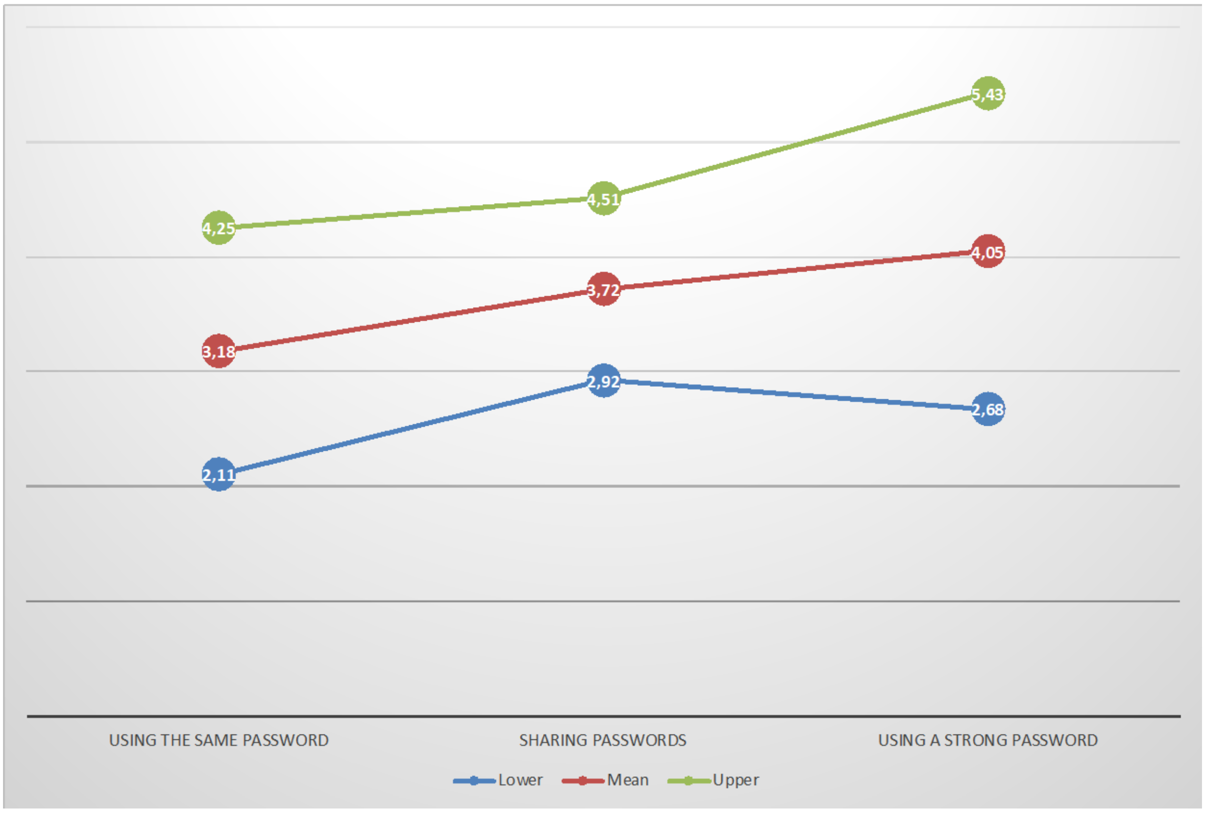


Figure 14: Password management (knowledge)

What respondents thought about the need to use strong passwords (attitude) is lower compared to their knowledge (3.49 as per Figure 15). The responses further indicate that respondents thought it was acceptable to use the same password for their social media platforms and work accounts.

A potential reason could be that the policies and procedures "*force*" behaviour of employees and could indicate that the organisations had potential good controls in place for these items to prevent incidents.

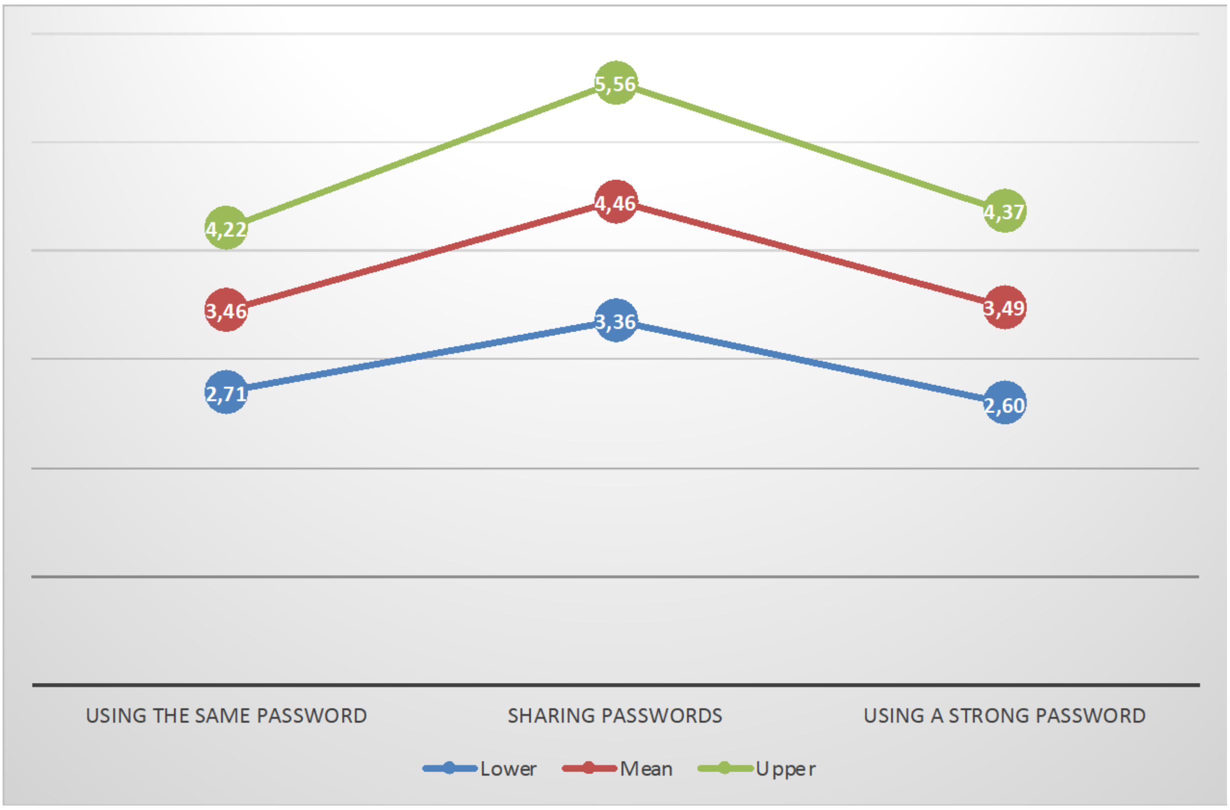


Figure 15: Password management (attitude)

The behaviour response was compared to validate whether they did indeed use the same password across many accounts (behaviour). As seen in Figure 16, the respondents indicated that their use of a different password was above their knowledge and behaviour scores (4.42), implying that the respondents' behaviour to some extent contradicted their knowledge and attitude towards these aspects.

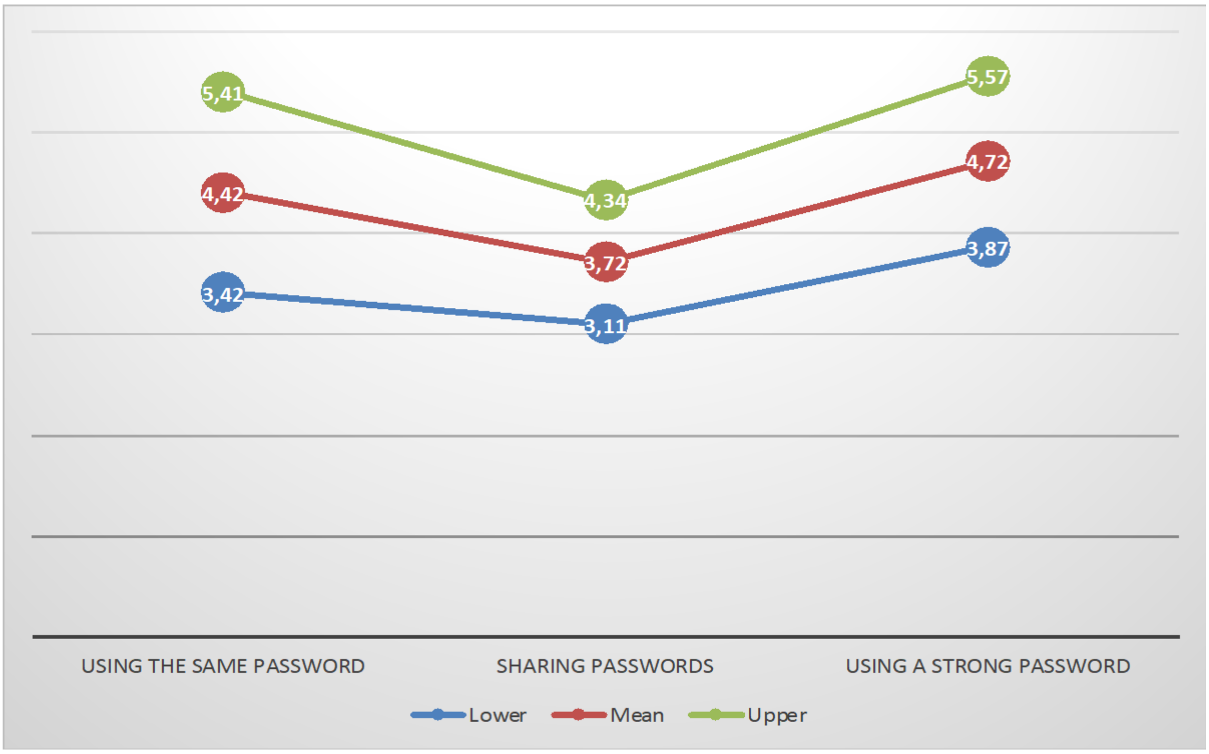


Figure 16: Password management (behaviour)

From Figure 16 there is a further trend indicating that respondents shared passwords with colleagues. This trend is a confirmation that there is a need for education to improve CSA on the safe use of passwords.

Email use

This section of the questionnaire tested the respondents' knowledge, attitude and behaviour of the guidelines pertaining to safe email usage. The questions posed to the participants are noted in Table 15.

Table 15: Email use questions (Parsons et al., 2017)

Focus area: ***Email use***	**Knowledge**	**Attitude**	**Behaviour**
Clicking on links in emails from known senders	I am allowed to click on any links in the emails from people I know.*	It's always safe to click on links in emails from people I know.*	I don't always click on links in emails just because they come from someone I know.
Clicking on links in emails from unknown senders	I am not permitted to click on a link in an email from an unknown sender.	Nothing bad can happen if I click on a link in an email from an unknown sender.*	If an email from an unknown sender looks interesting I click on a link within it.*
Opening attachments in emails from unknown senders	I am allowed to open an attachment from unknown senders.*	It's risky to open email attachments from an unknown sender.	I don't open email attachments if the sender is unknown to me.

*Reverse scoring was used to calculate the averages

The knowledge relating to the safe usage of email is depicted in Figure 17. The knowledge level relating to the treatment of emails from known senders is below 3 (2.85), whereas the treatment of emails and attachments from unknown senders scored above 3 (3.9 and 3.38, respectively). This indicates that the respondents did have knowledge relating to the handling of emails from unknown senders, but not from known senders.

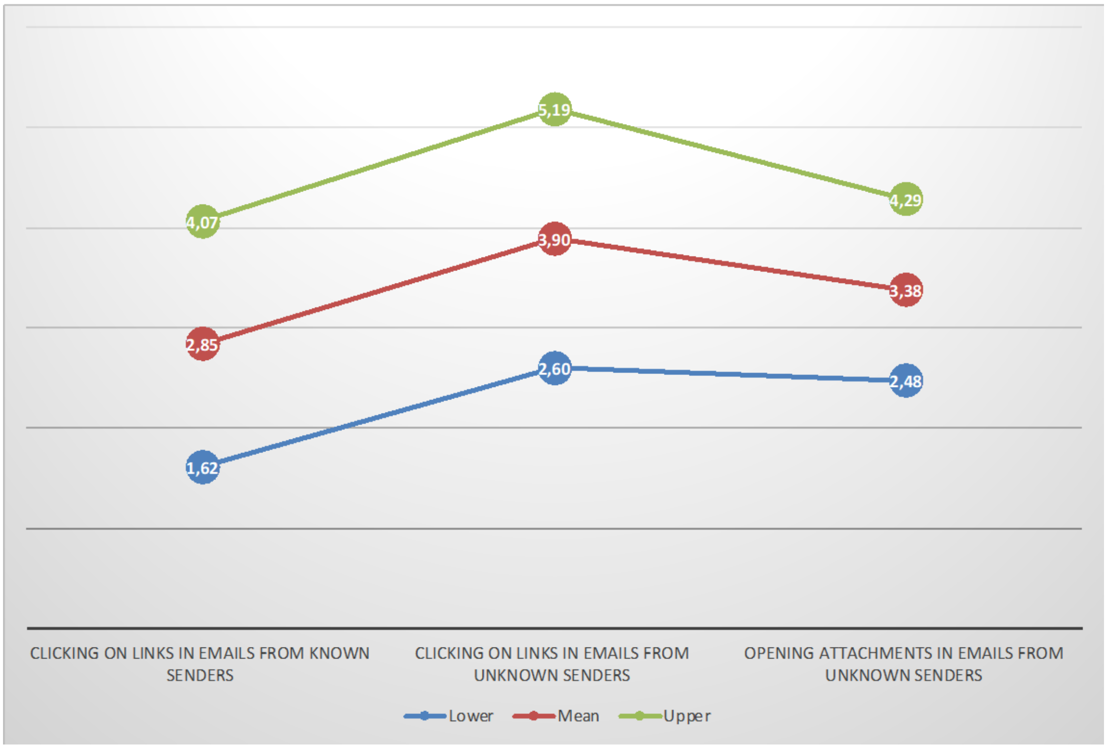


Figure 17: Email use (knowledge)

What respondents thought about the guidelines of email usage (attitude) aligns with their knowledge, where emails from unknown senders were treated with more care than emails from known senders, as shown in Figure 18. In the case of opening attachments in emails from unknown senders, the respondents' attitude scored higher than their knowledge. In the case of opening attachments from unknown senders and clicking on links received from unknown senders, the respondents acknowledged the risk.

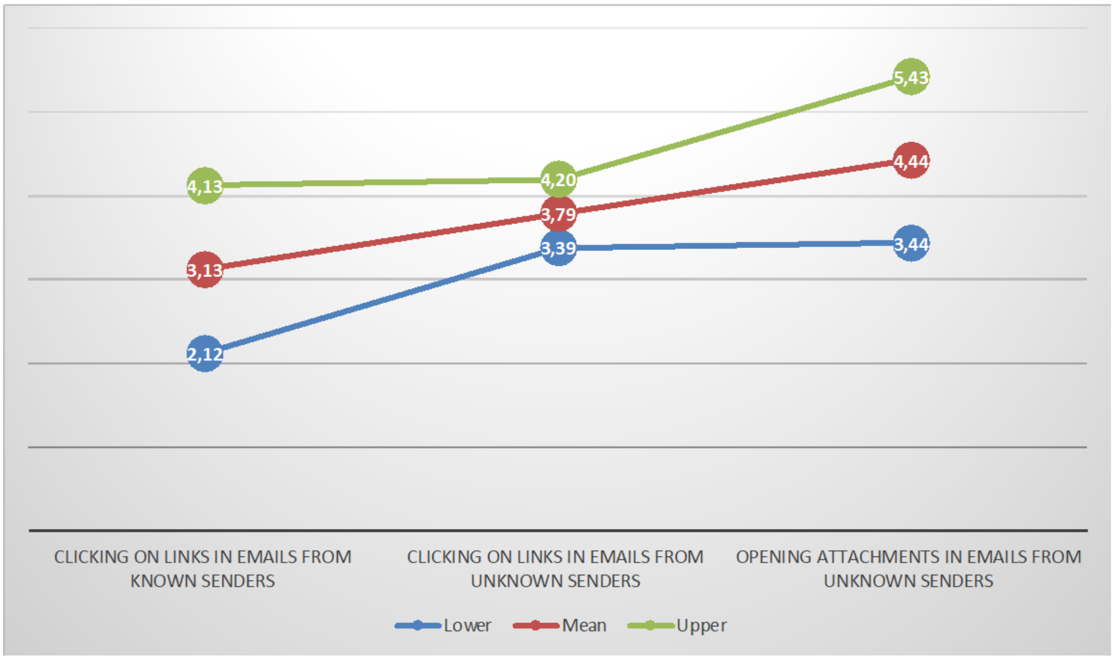


Figure 18: Email use (attitude)

The behaviour confirms that opening attachments from unknown senders was generally not done, and the potential of clicking on links from unknown senders was lower.

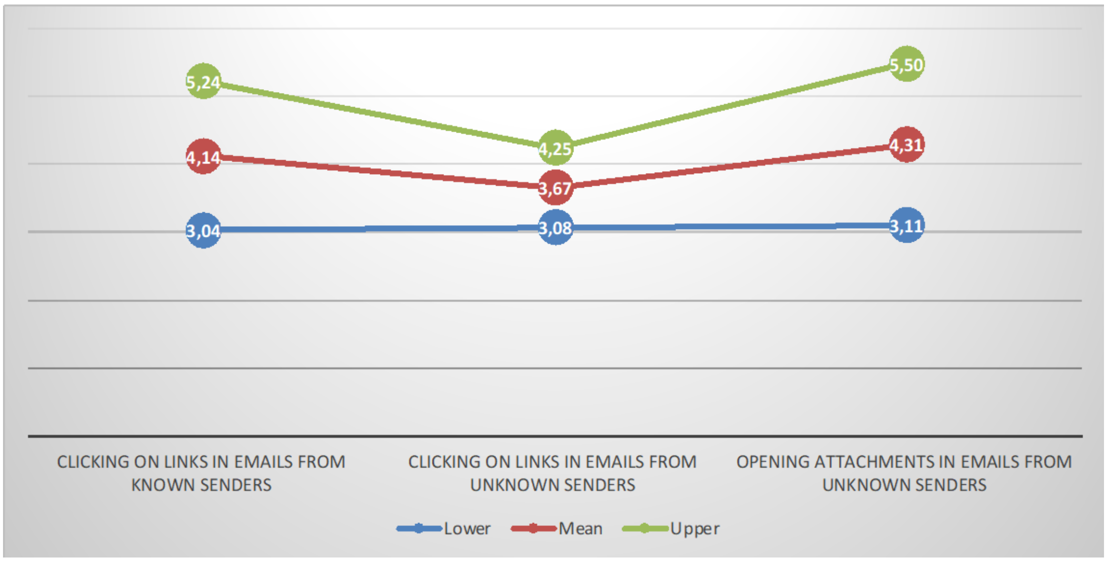


Figure 19: Email use (behaviour)

The risk of *clicking on links through emails* is a trend that needs education and training. Although the sample size was small and cannot be generalised, the trend of individuals being tricked to reveal personal information via fake emails and links has also been confirmed by Interpol as one of the top five cyberthreats in Africa (Interpol, 2021).

Internet use

This section of the questionnaire tested the respondents' knowledge of the guidelines pertaining to safe internet usage. The questions posed to the participants are noted in Table 16.

Table 16: Internet use questions (Parsons et al., 2017)

Focus area: ***Internet use***	**Knowledge**	**Attitude**	**Behaviour**
Downloading files	I am allowed to download any files onto my work computer if they help me to do my work. *	It can be risky to download files on my work computer.	I download any files onto my work computer that will help me get the job done. *
Accessing dubious websites	While I am at work, I shouldn't access certain websites.	Just because I can access a website at work, it doesn't mean it's safe.	When accessing the internet at work, I visit any website that I want to. *
Entering information online	I am allowed to enter any information on any website if it helps me do my job. *	If it helps me do my job, it doesn't matter what information I put on a website. *	I assess the safety of websites before entering information.

*Reverse scoring was used to calculate the averages

As with the usage of email, the respondents were knowledgeable about how they should engage with the internet. Figure 20 highlights the different knowledge levels. The respondents seemed to be prepared to download files from the internet if they needed them to do their work.

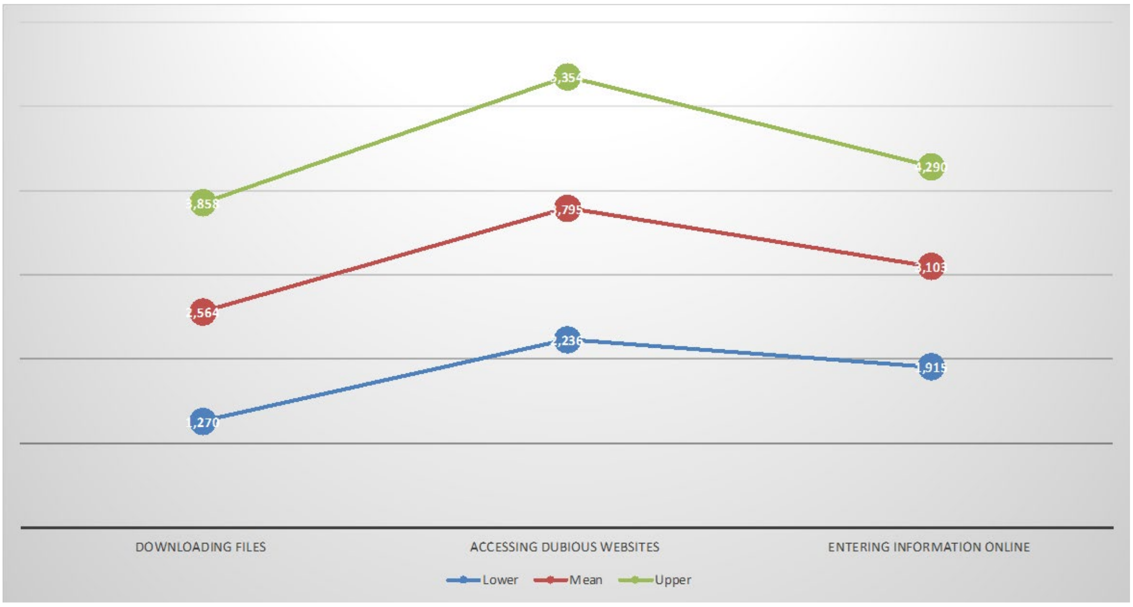


Figure 20: Internet use (knowledge)

There is also an indication they were prepared to enter their details on websites if they needed to get their job done, although the behaviour indicates that they would assess the safety of the website.

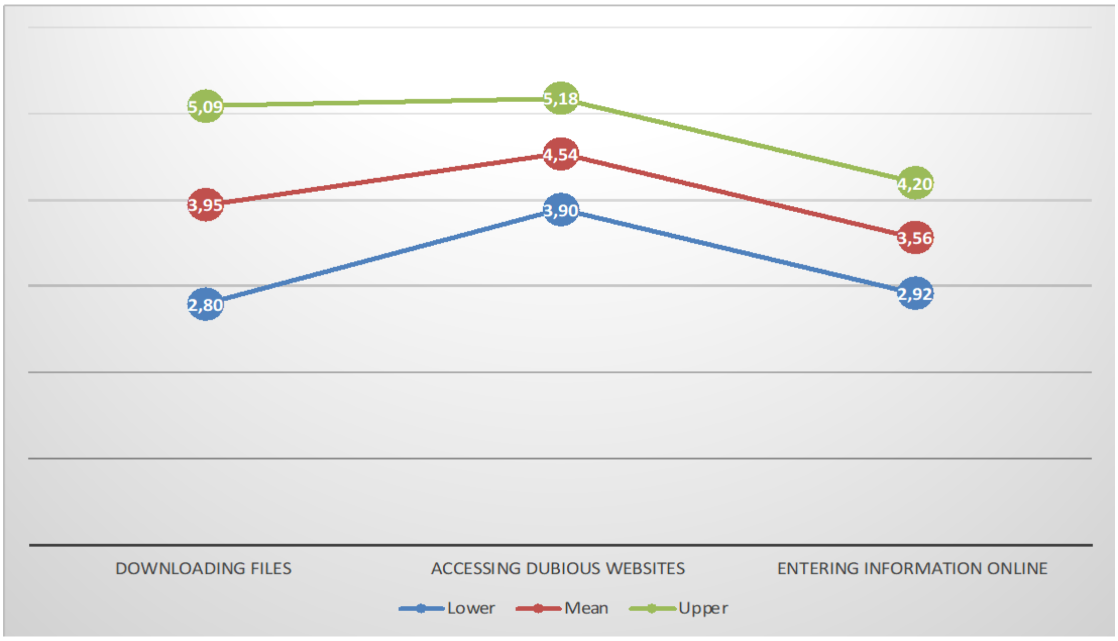


Figure 21: Internet use (attitude)

In contrast to the knowledge and attitude curves for safe internet usage, the behaviour related to entering information online was higher (4.19), which indicates that users do not tend to enter their information online.

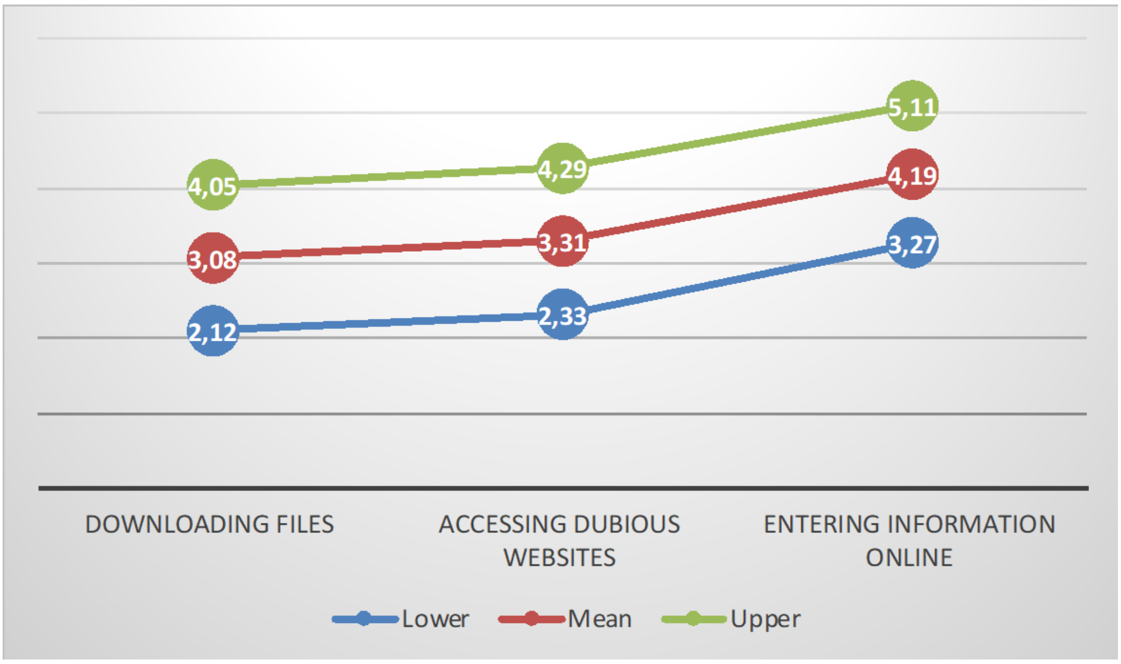


Figure 22: Internet use (behaviour)

From the results, it can be seen that there is a need for training on the downloading of files, as there is a knowledge gap in this area. It was confirmed that respondents would download files from the internet if they needed to get their work completed.

Social media use

This section of the questionnaire tested the respondents' knowledge, attitude and behaviour of the guidelines pertaining to social media usage. The questions posed to the participants are noted in Table 17.

Table 17: Social media use questions (Parsons et al., 2017)

Focus area: *Social media use*	**Knowledge**	**Attitude**	**Behaviour**
Social media privacy settings	I must periodically review the privacy settings on my social media accounts.	It's a good idea to regularly review my social media privacy settings.	I don't regularly review my social media privacy settings. *
Considering consequences	I can't be fired for something I post on social media. *	It doesn't matter if I post things on social media that I wouldn't normally say in public. *	I don't post anything on social media before considering any negative consequences.
Posting about work	I can post what I want about work on social media. *	It's risky to post certain information about work on social media.	I post whatever I want about my work on social media. *

*Reverse scoring was used to calculate the averages

The knowledge of social media usage indicates a potential knowledge gap when considering consequences during the use of social media as illustrated in Figure 23.

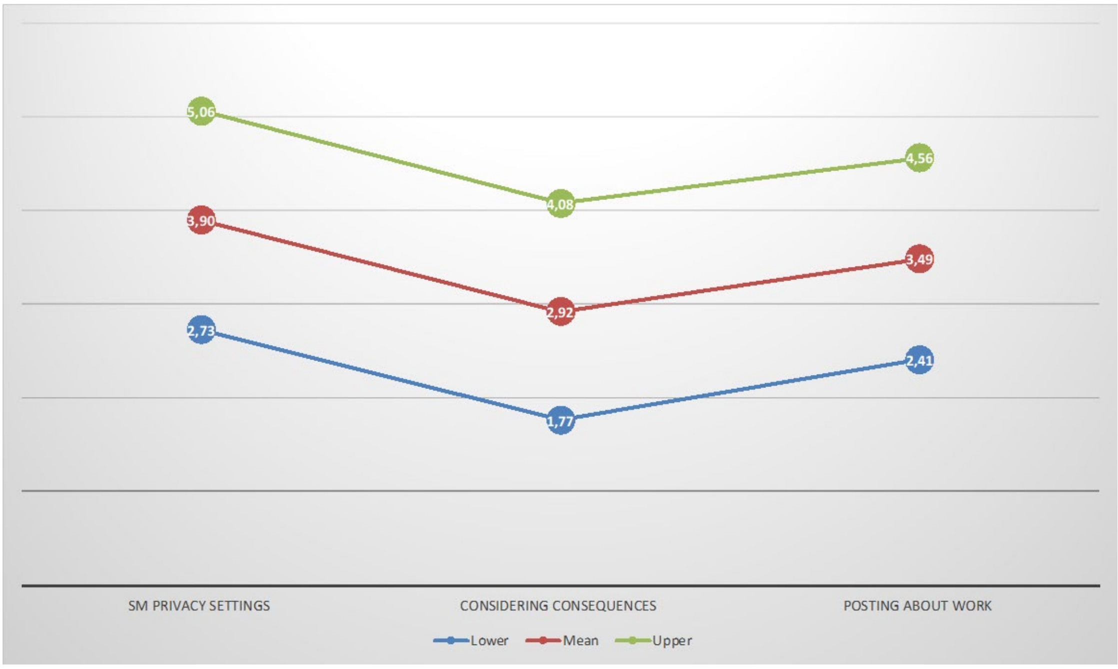


Figure 23: Social media use (knowledge)

If compared to what respondents thought about the guidelines of the knowledge they had, the pattern confirms a *knowledge gap* in guidelines on considering consequences during the use of social media. This is illustrated in Figure 24.

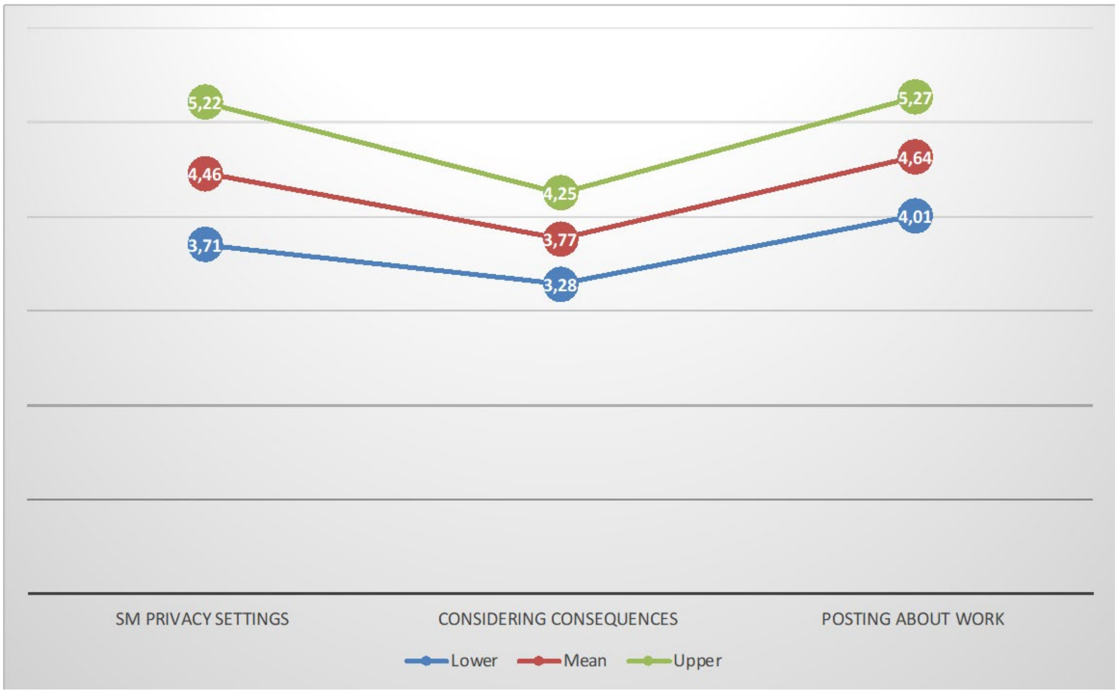


Figure 24: Social media use (attitude)

Looking at the behaviour patterns during social media usage, they indicate that respondents might not review the settings regularly as per Figure 25. This is contradictory to the respondents' confirmation that they knew that social media privacy settings should be regularly reviewed on their social media accounts.

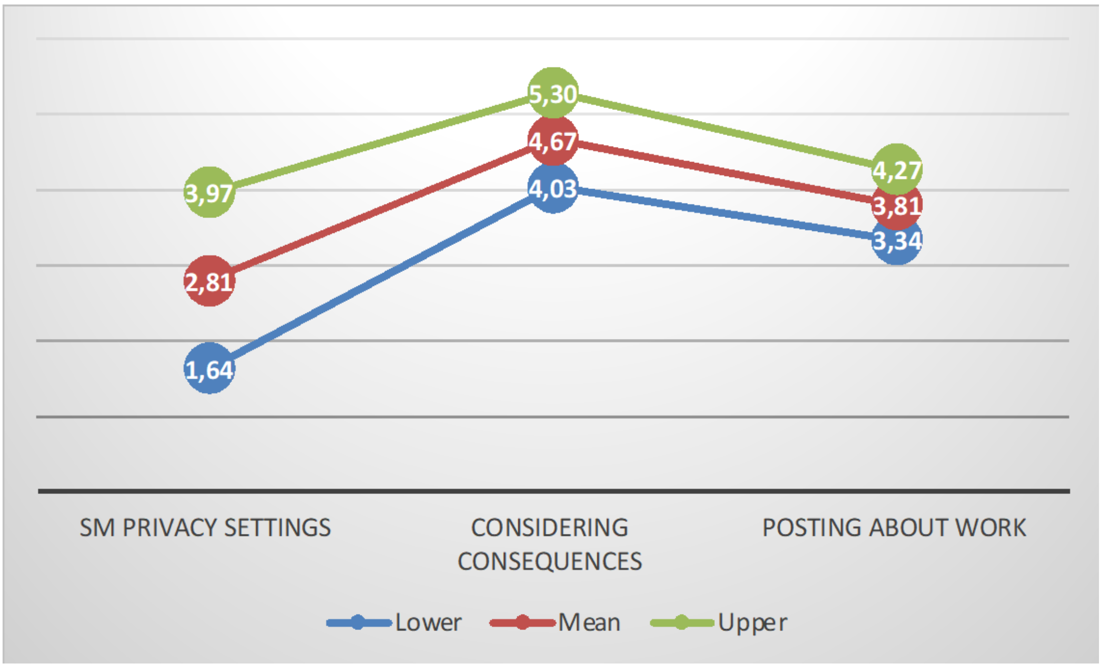


Figure 25: Social media use (behaviour)

Mobile devices

This section of the questionnaire tested the respondents' knowledge, attitude and behaviour of the guidelines pertaining to mobile device usage. The questions posed to the participants are noted in Table 18.

Table 18: Mobile device usage questions (Parsons et al., 2017)

Focus area: *Mobile device use*	**Knowledge**	**Attitude**	**Behaviour**
Physically securing mobile device	When working in a public place, I have to keep my laptop with me at all times.	When working in a café, it's safe to leave my laptop unattended for a minute. *	When working in a public place, I leave my laptop unattended.
Sending sensitive information via Wi-Fi	I am allowed to send sensitive work files via a public Wi-Fi network. *	It's risky to send sensitive work files using a public Wi-Fi network.	I send sensitive work files using a public Wi-Fi network. *
Shoulder surfing	When working on a sensitive document, I must ensure that strangers can't see my laptop screen.	It's risky to access sensitive work files on a laptop if strangers can see my screen.	I check that strangers can't see my laptop screen if I'm working on a sensitive document.

*Reverse scoring was used to calculate the averages

Generally the scores related to safe mobile device usage were high, with the exception of sending sensitive information via Wi-Fi.

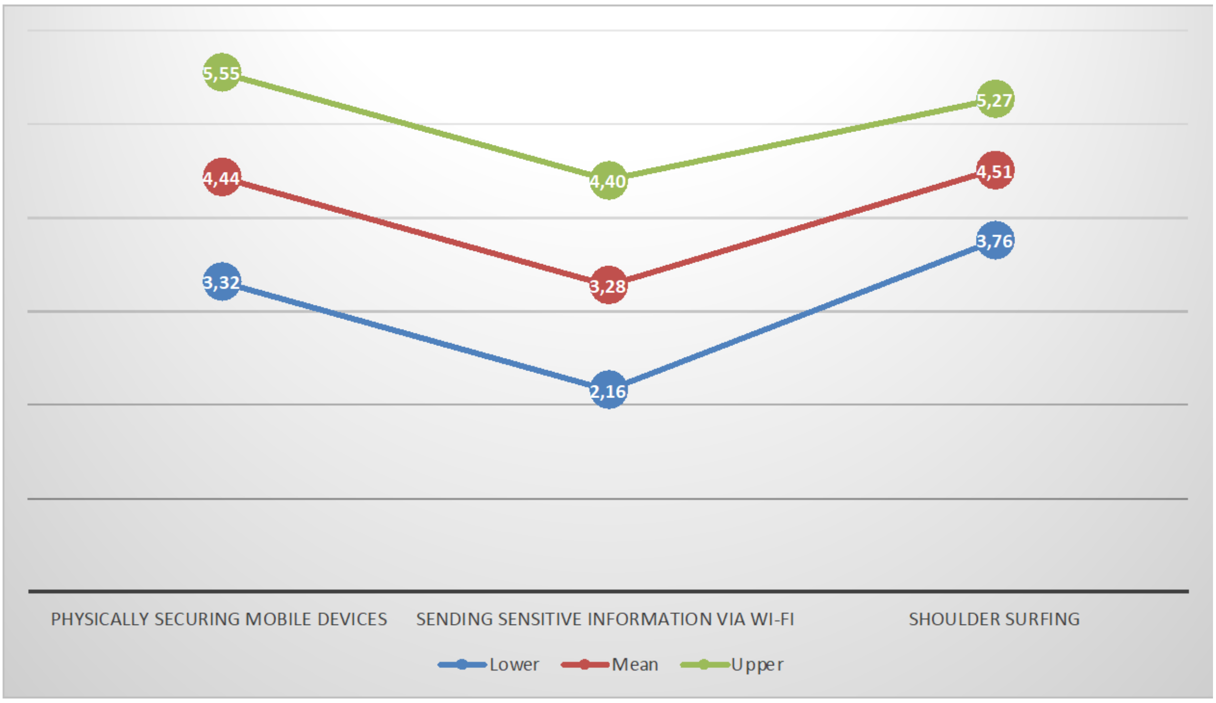


Figure 26: Mobile devices (knowledge)

Mobile device usage knowledge levels were high although the respondents were prepared to send sensitive data across a public Wi-Fi network (behaviour), even if they thought it was risky, as shown in Figure 27 indicating attitude.

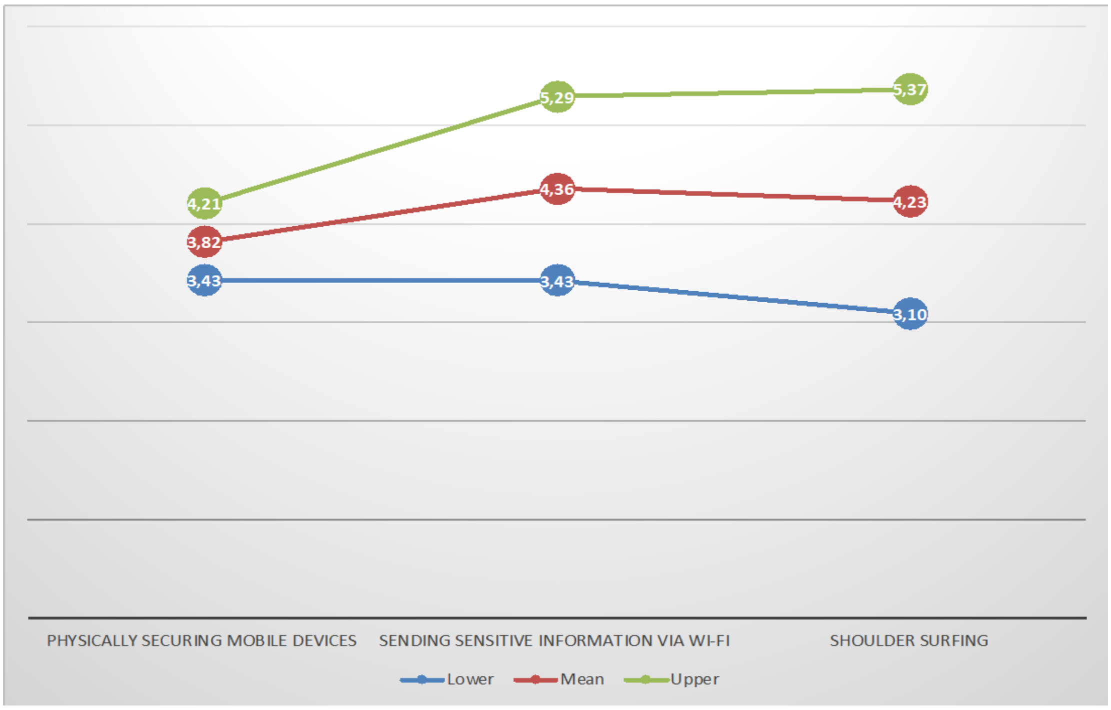


Figure 27: Mobile devices (attitude)

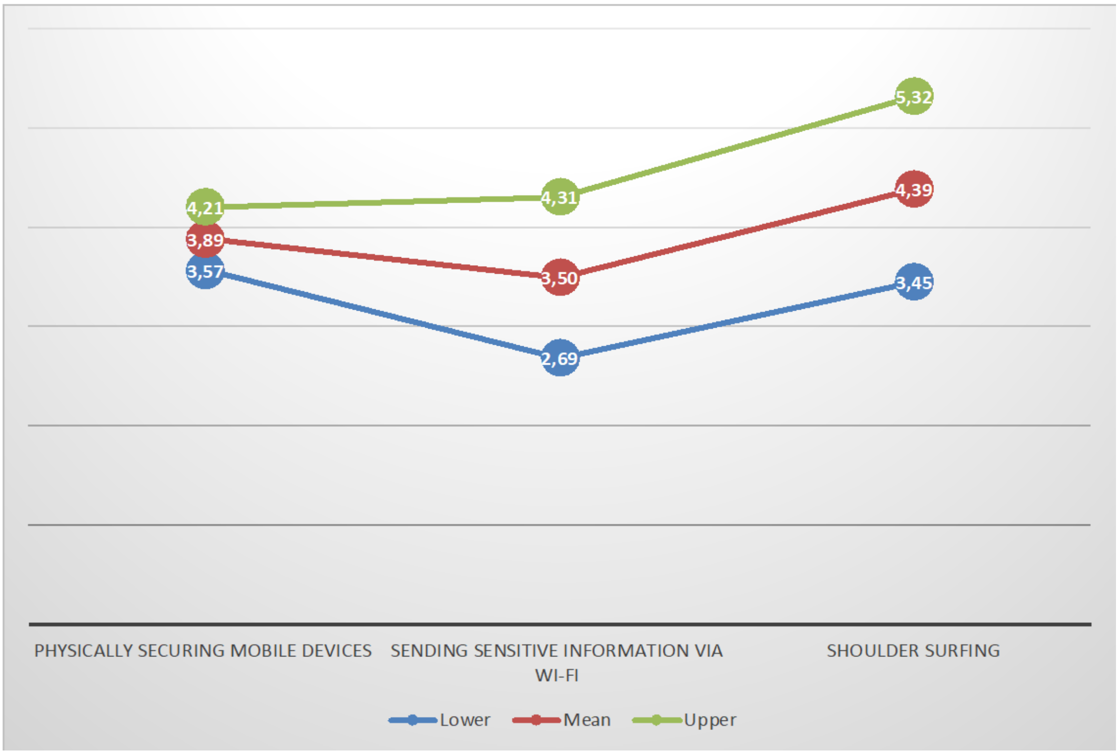


Figure 28: Mobile devices (behaviour)

The trend confirmed from the knowledge as well as attitude questions indicates a training and education gap regarding the sending of sensitive data across public Wi-Fi networks, as their behaviour confirmed that they would do this.

Information handling

This section of the questionnaire tested the respondents' knowledge of the guidelines pertaining to information handling. The questions posed to the participants are noted in Table 19.

Table 19: Information handling questions (Parsons et al., 2017)

Focus area: Information handling	**Knowledge**	**Attitude**	**Behaviour**
Disposing of sensitive print-outs	Sensitive print-outs can be disposed of in the same way as non-sensitive ones. *	Disposing of sensitive print-outs by putting them in the rubbish bin is safe. *	When sensitive print-outs need to be disposed of, I ensure that they are shredded or destroyed.
Inserting removable media	If I find a USB stick in a public place, I shouldn't plug it into my work computer.	If I find a USB stick in a public place, nothing bad can happen if I plug it into my work computer. *	I wouldn't plug a USB stick found in a public place into my work computer.
Leaving sensitive material	I am allowed to leave print-outs containing sensitive information on my desk overnight. *	It's risky to leave print-outs that contain sensitive information on my desk overnight.	I leave print-outs that contain sensitive information on my desk when I'm not there. *

*Reverse scoring was used to calculate the averages

Knowledge levels regarding safe information handling was low across all measurements. From Figure 29, the deviations show a very diverse response, indicating that the knowledge of the respondents was at different levels.

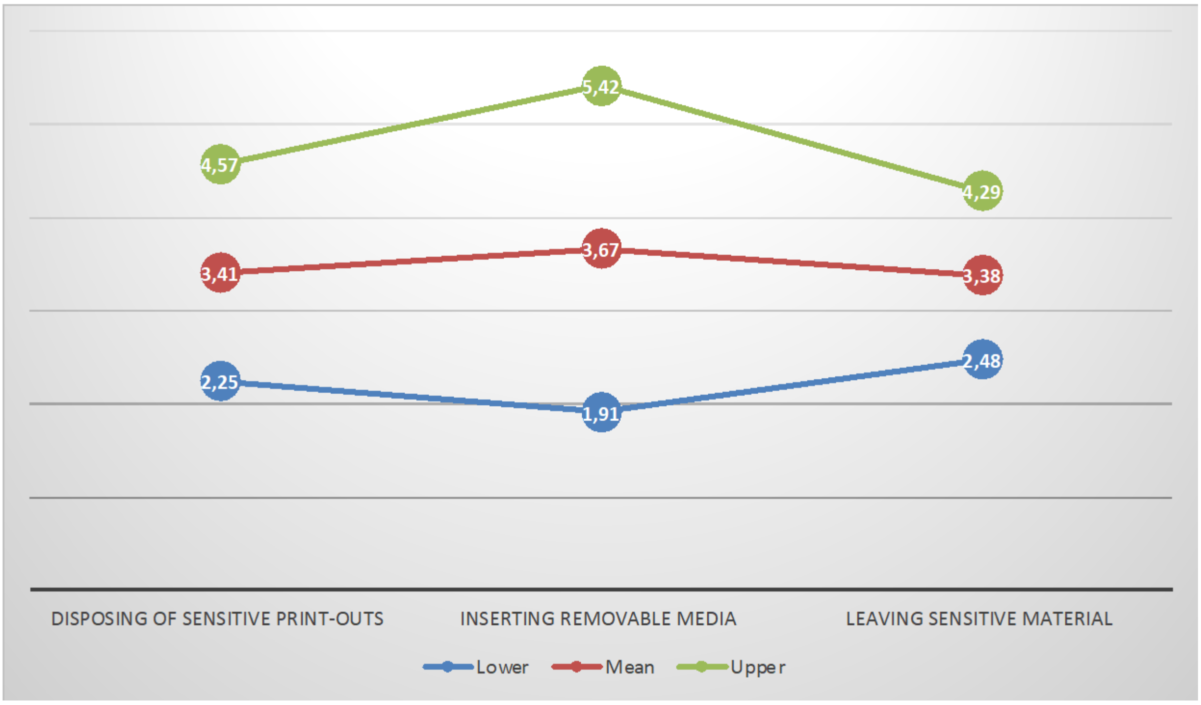


Figure 29: Information handling (knowledge)

The respondents' attitude relating to leaving sensitive information (4.49) was much higher than their knowledge (3.38) and behaviour (3.64) related to this topic.

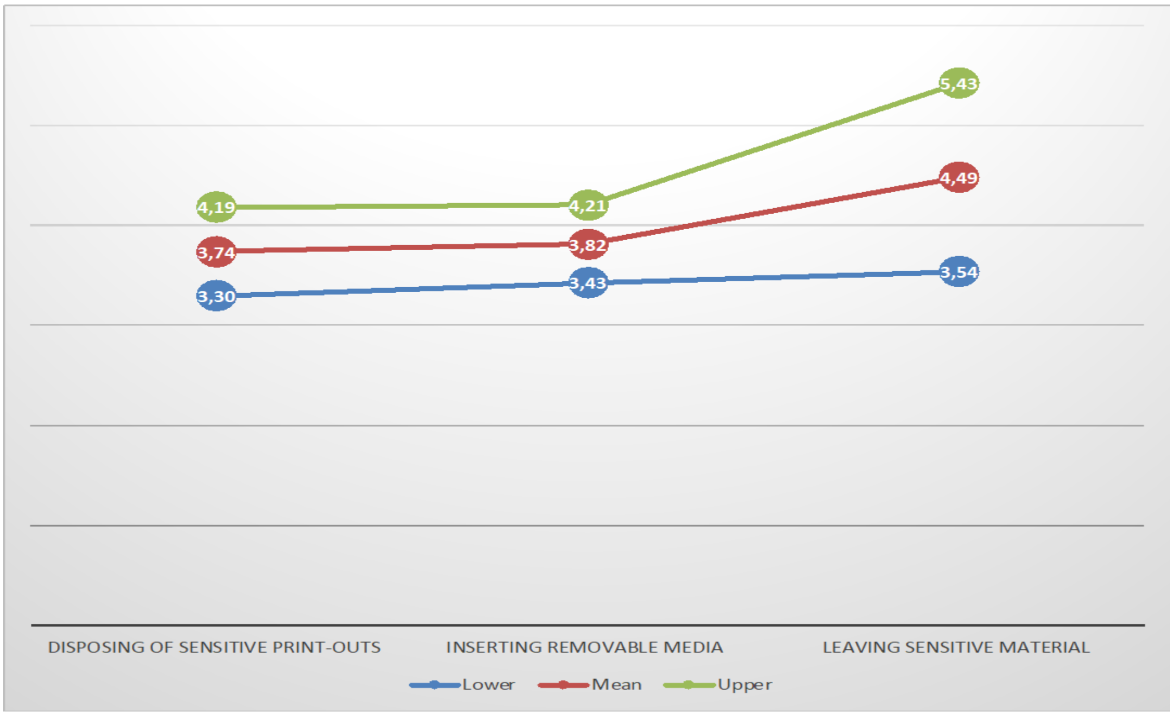


Figure 30: Information handling (attitude)

For information handling, the respondents' behaviour contradicts their knowledge level, which could indicate that there are controls in place forcing a certain behaviour.

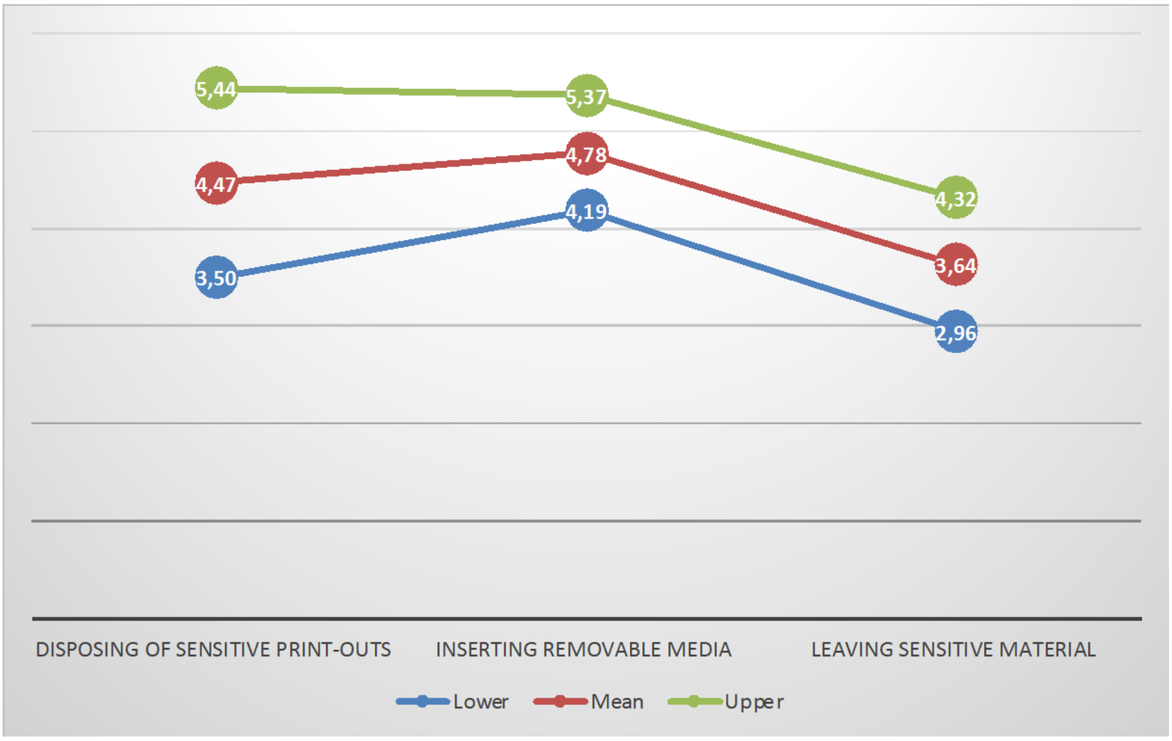


Figure 31: Information handling (behaviour)

Incident reporting

This section of the questionnaire tested the respondents' knowledge, attitude and behaviour of the guidelines pertaining to incident reporting. The questions posed to the participants are noted in Table 20.

Table 20: Incident reporting questions (Parsons et al., 2017)

Focus area: Incident reporting	**Knowledge**	**Attitude**	**Behaviour**
Reporting suspicious behaviour	If I see someone acting suspiciously in my workplace, I should report it.	If I ignore someone acting suspiciously in my workplace, nothing bad can happen. *	If I saw someone acting suspiciously in my workplace, I would do something about it.
Ignoring poor security behaviour by colleagues	I must not ignore poor security behaviour by my colleagues.	Nothing bad can happen if I ignore poor security behaviour by a colleague. *	If I noticed my colleague ignoring security rules, I wouldn't take any action. *
Reporting all incidents	It's optional to report security incidents. *	It's risky to ignore security incidents, even if I think they're not significant.	If I noticed a security rules incident, I would report it.

*Reverse scoring was used to calculate the averages

Incident reporting is an important communication mechanism in cybersecurity reporting. From the knowledge levels, it is clear that there was a very diverse set of responses and that respondents did not generally report incidents or poor behaviour of colleagues.

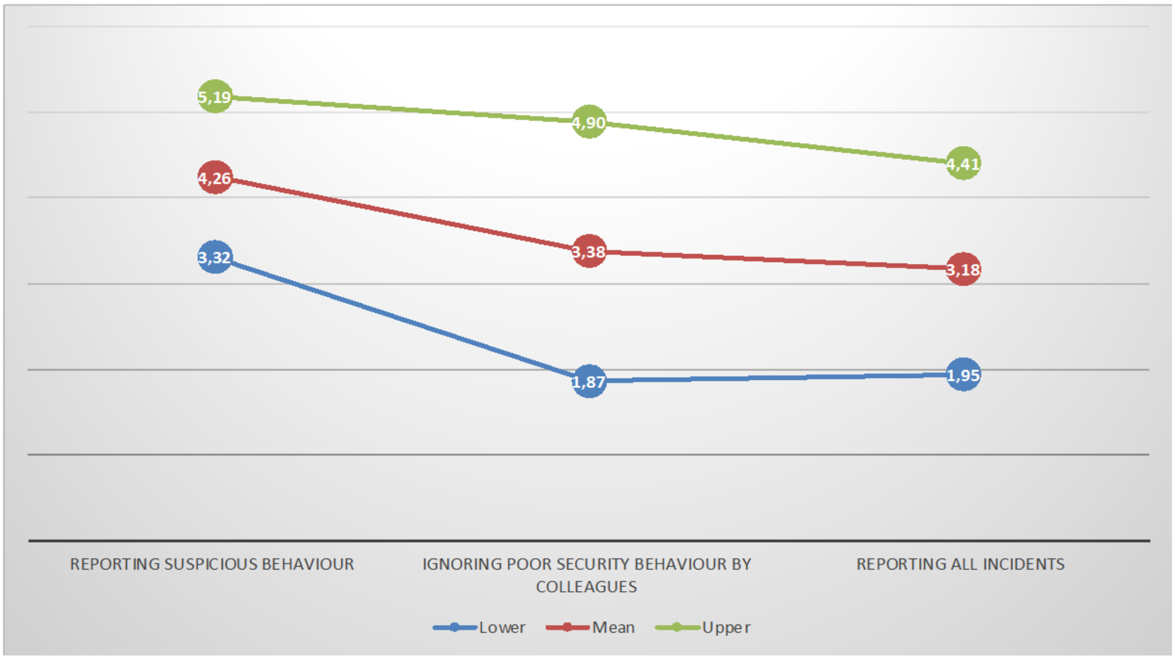


Figure 32: Incident reporting (knowledge)

If what the respondents' think (attitude) is compared to what they do (behaviour), then there is some agreement that suspicious incidents would be reported.

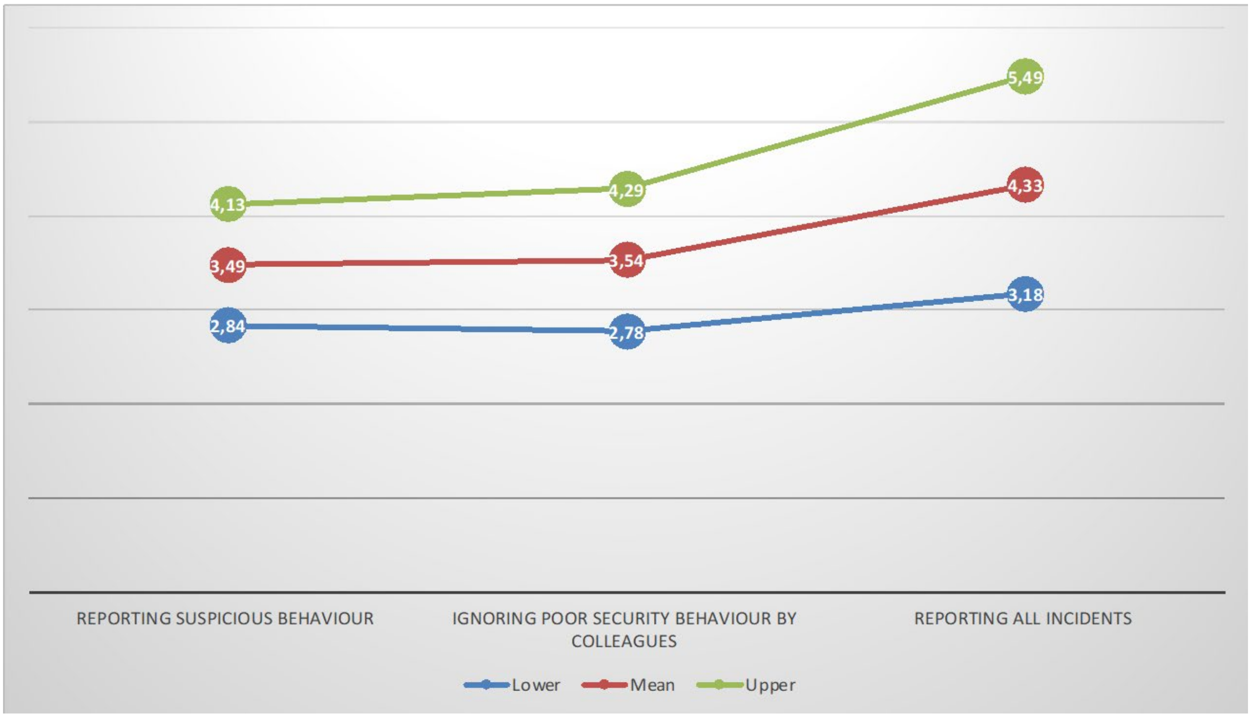


Figure 33: Incident reporting (attitude)

When it comes to inside the organisation and reporting colleagues' behaviour, there is a clear trend that this is not done.

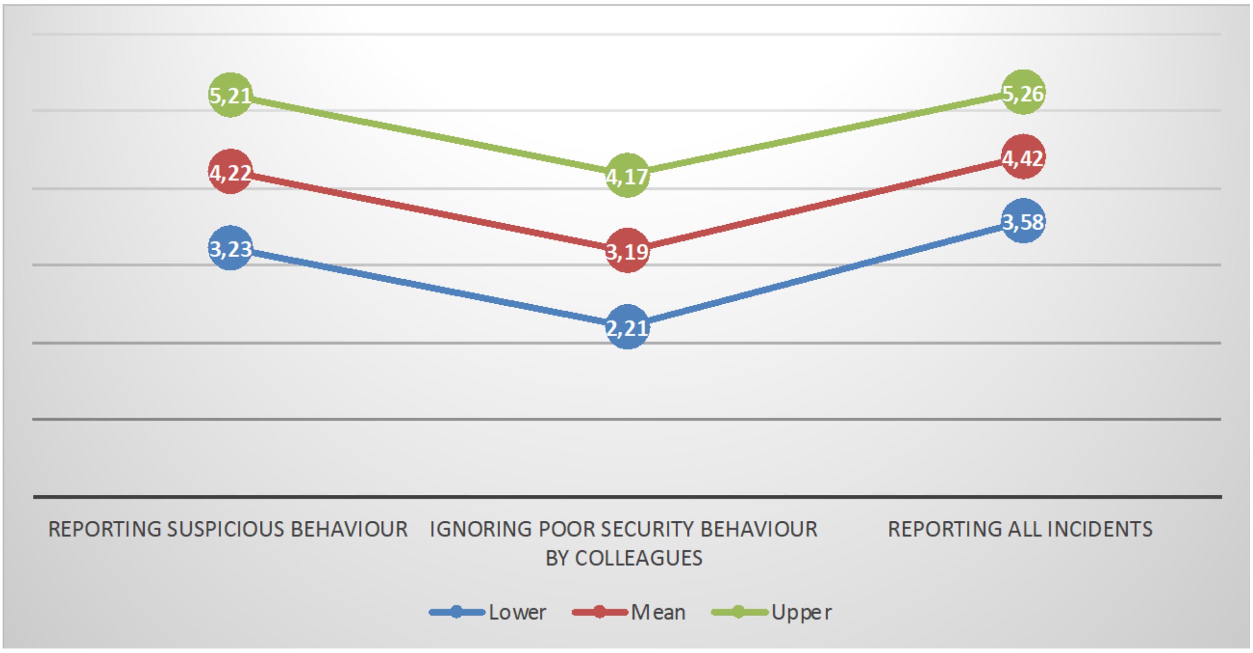


Figure 34: Incident reporting (behaviour)

This needs significant education and training as many cybersecurity incidents are from a human link inside an organisation.

For the comparison between the different aspects, the mean score across each aspect was calculated for knowledge, attitude and behaviour. The results are depicted in Figure 35. For password management, incident reporting, information handling and email use, the mean score for behaviour was higher than for knowledge and attitude.

A study in Australia (with 500 employees) indicated that knowledge of policy and procedures had a stronger influence on attitude towards policy and procedure than self-reported behaviour. The authors suggested that training and education would be more effective if it outlined not only what is expected (knowledge), but also provided an understanding of why this is important (attitude) (Parsons et al., 2014).

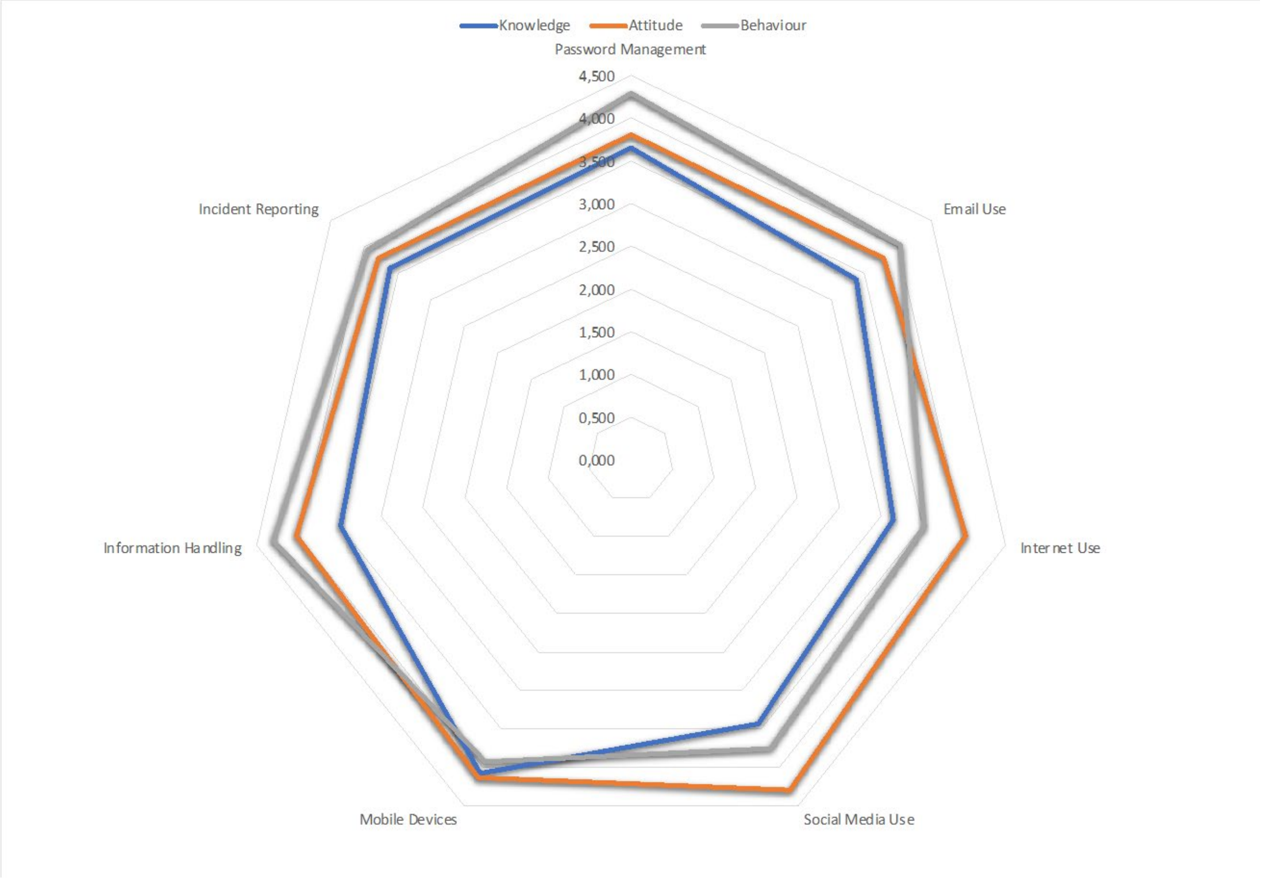


Figure 35: Comparison of knowledge, attitude and behaviour

From the data analysis, the summary of education and training needs is presented in Table 21. Training and education on cybersecurity risks is continuous. With digitalisation or the organisational landscape, the seven aspects are expected to increase to more than the current measures in the questionnaire. It is suggested that based on employee role and responsibility, focus areas of education should be identified and continuously built on. Reporting could also be driven from a behaviour perspective by introducing communication programmes of reporting in the organisation to share these incidents and not just follow an education approach.

Table 21: Education and training needs

	Knowledge	Attitude	Behaviour
Password management	Requires training	Requires training	Requires training
Email use	Requires training	Requires training	Requires training
Internet use	Requires training	Attitude level acceptable	Requires training
Social media use	Requires training	Attitude level acceptable	Requires training
Mobile devices	Requires training	Requires training	Requires training
Informational handling	Requires training	Attitude level acceptable	Requires training
Incident reporting	Requires training	Attitude level acceptable	Requires training

The above table can be used as a guideline for the topics which need to be prioritised for training. The subsequent chapter includes the details on the construction of training and education material for the improvement of baseline cybersecurity knowledge.

5 CONSTRUCTION OF TRAINING AND EDUCATION MATERIAL FOR BASELINE CYBERSECURITY KNOWLEDGE

5.1 Motivation for open-source training content

Chapter 2 presents a framework for identifying the minimum cybersecurity knowledge required by a typical employee in the water sector. Chapter 4 presents the baseline CSA levels based on the results of the HAIS-Q of a typical employee in the water sector. These two results are combined and a table is presented in this chapter which lists free online training courses on cybersecurity.

The Water Research Commission published the Water Research Development and Innovation Roadmap Skills Mapping Study, Volume 3: Short Course Skills Mapping Study in 2021 (Nel et al., 2021). This document identifies the needs and interventions relating to the supply of and demand for short courses for the water community. It comments on the importance of short courses for employees, which includes skills development and the inclusion of new technologies. The document also lists barriers to enrolment for potential short course participants, which include:

- Lack of funding
- Time and cost
- Long and cumbersome approval process

These barriers to enrolment support the utilisation of free online training courses on cybersecurity, as the sector can support employees in developing their CSA without incurring additional costs or requiring approval processes. The open-source learning material identified in this chapter therefore focuses on professional training material which is provided free of charge to any person who wishes to improve their CSA levels. By utilising these available courses, the development towards a cybersecure culture can be promoted within an organisation.

5.2 Training material table

From the framework presented in Chapter 2, it can be seen that training must be conducted at an individual level as well as an organisational level. In addition, the framework emphasises the following areas:

- Skills and knowledge
- Training
- Culture
- Awareness

The training material presented in this chapter is collated for the water sector employees on the topics identified in the framework and also the results of the HAIS-Q cybersecurity awareness results presented in Chapter 4, which include the areas of internet use, email use, social networking, password management, information handling and mobile computing. As cybersecurity knowledge is general knowledge, there is no need to produce specialised or new training material and employees are not required to complete formal short courses or certifications on the topics.

The complete training material table is listed in Table 22 below. The table provides information in the following columns:

- **Type of threat**: This names the cybersecurity threat. These names link to the CSA framework presented in Chapter 2.
- **Building the knowledge**: This provides information on the outcome of the training.
- **Training description**: This provides a brief overview of the training.
- **Training type**: This describes how the training will be presented.
- **Link to course**: This provides the hyperlink to the course content.

Table 22: Complete list of training material

Introduction: https://fedvte.usalearning.gov/publiccourses/critical101/index.htm?track=trackingon

INDIVIDUAL: SKILLS AND KNOWLEDGE				
Type of threat	**Building the knowledge**	**Training description**	**Training type**	**Link to course**
SECURITY BREACHES	Capacity to detect and report attacks	The course covers the threats and vulnerabilities faced when working within government systems. It provides a working knowledge of cyberintrusion methods and cybersecurity countermeasures to assist employees in preventing cyberattacks and protecting their systems and information.	Read and watch video	https://securityawareness.usalearning.gov/cybersecurity/index.htm#
NEGLIGENCE	Diagnostic abilities to anticipate, spot and react	Module 01 covers the ability to identify the computer's component layers and associated functions. Module 02 deals with the ability to recognise virtualisation concepts. Module 03 covers the ability to choose the correct security protection associated with a computer's component layer.	Read and watch video	https://www.dni.gov/ncsc/e-Learning_CyberExplore/index.html
SOCIAL ENGINEERING	Know the types of attackers, their motivation, resources and knowledge/skills	The extract covers the list of different hackers, their motivation and objectives.	Read document	https://securitystudio.com/social-engineering-attacks/
DENIAL OF SERVICE		The course provides an introduction to methods that hackers might use to access a computer system or network and deny authorised users access.	Read and do activities	https://www.dni.gov/ncsc/e-Learning_CyberExploits/module-1.html
	Know the different types of attacks	This training video closely examines the top ten cyberattacks that can affect an individual, or a large business, depending on the scale.	Watch video	https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks?source=sl_frs_nav_playlist_video_clicked
MALICIOUS INSIDER		This course provides a thorough understanding of how insider threat awareness is an essential component of a comprehensive security programme.	Read, watch video and do activities	https://securityawareness.usalearning.gov/itawareness/index.htm
MALWARE/ RANSOMEWARE	Grasp possible loopholes and risks	This video lesson guides learners through an attack and discusses what they need to know to protect themselves.	Watch video	https://www.cdse.edu/Training/Security-Training-Videos/Cybersecurity-Security/Ransomware/

STOLEN CREDENTIALS & UNAUTHORISED ACCESS	Recognise potential security threat, foresee impact and initiate suitable responses	Learners will learn how to identify, address and prevent a broad range of threats and attacks, while building an in-depth knowledge of essential cybersecurity terminology.	Read, watch video and do activities	Step 1: Sign Up: Join eLearning College Step 2: Log In: eLearningCollege | Login

ORGANISATIONAL: SKILLS AND KNOWLEDGE

Types of threats	Building the knowledge	Training description	Training type	Link to course
SECURITY BREACHES	Organisational cybersecurity capability	This course deals with how to protect and defend an organisation's network.	Read and watch video	https://skillsforall.com/launch?id=7662b32f-0a49-4d7a-b881-498eb3be42cc
NEGLIGENCE		The training tutorial is aimed at equiping learners with the necessary skills to pick up suspicious emails.	Watch video	https://securityawareness.usalearning.gov/cdse/multimedia/shorts/dss_cie_fy12/story_html5.html
SOCIAL ENGINEERING	Organisation's ability to detect and respond in critical situations	This game-based training focuses on the detection of malicious websites, infected devices, breaches, phishing emails, social engineering and other common attacks. The game can be a good training tool to help develop rapid response in critical situations.	Watch video and play a game	http://targetedattacks.trendmicro.com/
DENIAL OF SERVICE **MALICIOUS INSIDER**	Interorganisational knowledge sharing	The training introduces why cybersecurity is important and how attacks happen, and then covers key areas with tips that complement any existing policies and procedures.	Read and watch video	https://www.ncsc.gov.uk/training/top-tips-for-staff-scorm-v2/scormcontent/index.html#/lessons/OKuYXwN7uEicNmRDP0uI4M4oWefFjjCG
MALWARE/ RANSOMEWARE **STOLEN CREDENTIALS & UNAUTHORISED ACCESS**	Develop cybersecurity policies to make employees knowledgeable	This 15-minute training covers secure communication, data classification, phishing, physical security, social engineering, data privacy, third-party/application security, laptop standard, protecting data and acceptable use. There is no assessment component.	Read and watch video	https://learnsecurity.amazon.com/training/story.html

INDIVIDUAL: TRAINING				
Types of threats	**Building the knowledge**	**Training description**	**Training type**	**Link to course**
SECURITY BREACHES	Training through gamification	The aim of the game is to promote CSA. Users need to answer relevant cybersecurity questions.	Play a game	https://keeptraditionsecure.tamu.edu/web/location/evans/
NEGLIGENCE	Develop ability to manage incidents and reduce successful attacks	Explore how a threat-informed mindset can help focus efforts on improving and understanding how defences fare against real-world adversaries.	Read and do activities	https://www.cybrary.it/course/mitre-attack-defender-mad-attack-fundamentals
SOCIAL ENGINEERING		The training provides approaches to follow in defending against phishing.	Read and watch video	https://www.ncsc.gov.uk/training/top-tips-for-staff-scorm-v2/scormcontent/index.html#/lessons/CCcwL5ktLwgz-pObLag2QpUNeClHVQ61
	Recognise threats and take appropriate action to reduce the cyber-risk	This tutorial covers what a ransomware attack is, how it works and how to protect against it.	Read and watch video	https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-ransomware-attack?source=sl_frs_nav_playlist_video_clicked
DENIAL OF SERVICE		In this video training, a simulation on a command-and-control situation is implemented to uncover suspicious activity by using Devo Security Operations (SecOps).	Read and watch video	https://docs.devo.com/confluence/ndt/latest/applications/devo-security-operations/use-cases/command-control#44290010e0b97ee239ed457aaca7c6ca2f4bc64e
MALICIOUS INSIDER	Use cyber-ranges to learn new techniques	In this game, the user is challenged to lead cybersecurity against increasingly gradual attacks by reinforcing the defences to ward off attacks in diverse challenges that involve breaking passwords, codes and confidential information.	Play a game	https://www.pbs.org/wgbh/nova/labs/lab/cyber/#
MALWARE/ RANSOMEWARE	Hands-on skills training	This one-hour training is geared toward government employees of any nation. It covers cybersecurity basics, threats, online safety, protecting government information and mobile device security.	Watch a video	https://cybilportal.org/webinars/cybersecurity-fundamentals-training-for-government-employees/

STOLEN CREDENTIALS/ UAUTHORISED ACCESS	Build capability of spotting potential cyberthreats and preparedness to respond in an adequate manner	Learners learn about the different cyberattacks and methods of dealing with the threats.	Read and do activities	https://onlinecourses.swayam2.ac.in/cec22_cs03/unit?unit=25&lesson=35

ORGANISATIONAL: TRAINING				
Types of threats	**Building the knowledge**	**Training description**	**Training type**	**Link to course**
SECURITY BREACHES	Build capacity to detect and report attacks	This course covers the foundations, processes and outcomes from ethical hacking and common attacks that demand this skill to be acquired.	Read and watch video	Step 1: Sign Up: greatlearning (mygreatlearning.com) Step 2: Log In: Greatlearning login (mygreatlearning.com)
NEGLIGENCE		The training focuses on the importance of keeping devices secure.	Read and do activities	https://www.ncsc.gov.uk/training/top-tips-for-staff-scorm-v2/scormcontent/index.html#/lessons/87ugPyVHNVvMOJVzYo7so3o1_SHTztLY
SOCIAL ENGINEERING	Training must be tailored to meet the security policies of the organisation	This course deals with the influence and impact of and the need for cybersecurity when defending the critical infrastructure and key resources.	Read and watch video	https://fedvte.usalearning.gov/publiccourses/critical101/index.htm?track=trackingon
DENIAL OF SERVICE				

INDIVIDUAL: CULTURE				
Types of threats	**Building the knowledge**	**Training description**	**Training type**	**Link to course**
SECURITY BREACHES	Prevent security breaches by ensuring employee compliance with security policies	This game-based training provides the learners with the ablility to ensure compliance.	Read and play a game	https://securityawareness.usalearning.gov/cdse/multimedia/games/TomorrowsInternet/story.html
NEGLIGENCE		This training explains the importance of reporting cyberincidents.	Read and do activities	https://www.ncsc.gov.uk/training/top-tips-for-staff-scorm-v2/scormcontent/index.html#/lessons/WYmLWn9RxM5rwdOcGzPZFHQtPS0FwYHV

ORGANISATIONAL: CULTURE				
Types of threats	**Building the knowledge**	**Training description**	**Training type**	**Link to course**
SECURITY BREACHES	Create and maintain a culture of security awareness	The training tutorial equips learners with the necessary tools for being aware of security threats.	Read and do activities	https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:online-data-security
NEGLIGENCE		The training is aimed at developing behaviour of protecting classified information.	Watch a video	https://securityawareness.usalearning.gov/cdse/multimedia/shorts/spills/Block10/Introduction/page_0010.html
	Culture of excellent security practices can be fostered through ongoing training and awareness	This training is aimed at improving the level of security awareness and ability to recognise and report attacks or suspicious activities.	Play a game	https://www.infosecinstitute.com/iq/choose-your-own-adventure/?utm_source=resources&utm_medium=infosec%20network&utm_campaign=cyoa&utm_content=main&utm_term=awareness
SOCIAL ENGINEERING		The training focuses on creating a workplace cybersecurity culture.	Play a video	https://cdse.acms.com/pksulmr53tsf/
DENIAL OF SERVICE	Minimise risks from humans by promoting security culture	The course covers the type of cyberintelligence required in order to promote a security culture.	Read and watch video	https://fedvte.usalearning.gov/publiccourses/ici/iciframe.php

MALICIOUS INSIDER		Employees are an organisation's first line of defence against threats to the mission or to the safety of the workforce. To motivate employees to actively participate in security and safety initiatives, organisational leaders must create an environment in which personnel trust leadership to be fair, honest and transparent.	Read and watch video	https://securityawareness.usalearning.gov/maximizing-trust/index.htm
MALWARE/ RANSOMEWARE	Cybersecurity culture can be embedded by regular communication, awareness, training and education initiatives	Cybersecurity threats and governance become crucial in promoting a security culture.	Read and do activities	Step 1: Sign Up: greatlearning (mygreatlearning.com) Step 2: Log In: Greatlearning login (mygreatlearning.com)
STOLEN CREDENTIALS/ UNAUTHORISED ACCESS		This training provides insight into how to improve passwords to avoid unauthorised access.	Read and do activities	https://www.ncsc.gov.uk/training/top-tips-for-staff-scorm-v2/scormcontent/index.html#/lessons/WYmLWn9RxM5rwdOcGzPZFHQtPS0FwYHV

INDIVIDUAL: AWARENESS				
Types of threats	**Building the knowledge**	**Training description**	**Training type**	**Link to course**
SECURITY BREACHES	Potential cyberthreat awareness	This module introduces learners to awarnesss of different cyberthreats.	Read and watch video	https://www.dni.gov/ncsc/e-Learning_CyberAware/index.html
NEGLIGENCE				
SOCIAL ENGINEERING	Situational awareness	This course gives learners simple but effective advice and techniques to improve situational awareness.	Read and do activities	http://content.greymatterlearning.co.uk/learning/Personal+Safety+Public+Version/index.html#/lessons/gXVlAX1SFrN1NqwJF22S6yeiMgNoB2Dz
DENIAL OF SERVICE	Awareness on creating strong passwords	This course provides an overview of current cybersecurity threats and best practices to keep information and information systems secure at home and at work. The training also reinforces best practices to protect classified information, controlled unclassified information and personally identifiable information.	Read and watch a video	https://cdse.usalearning.gov/course/view.php?id=371
MALICIOUS INSIDER		This course provides a thorough understanding of how insider threat awareness is an essential component of a comprehensive security programme, with the theme of "if you see something, say something".	Read and watch videos	https://securityawareness.usalearning.gov/itawareness/index.htm
MALWARE/ RANSOMEWARE	Developing critical awareness based on experiences of co-workers	Learners will understand what a ransomware attack is, how it works and how to protect against it.	Read and watch videos	https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-ransomware-attack?source=sl_frs_nav_playlist_video_clicked
ORGANISATIONAL: AWARENESS				
Types of threats	**Building the knowledge**	**Training description**	**Training type**	**Link to course**
SECURITY BREACHES		This course begins with a short test of the learner’s awareness and application of basic insider threat awareness skills. Learners who	Read and watch a video	https://cdse.usalearning.gov/course/view.php?id=840

	Design cybersecurity awareness to create compliant behaviours	successfully complete this test are not required to complete the course content and can proceed to print a Certificate of Completion.		
NEGLIGENCE		This video lesson explores the risks associated with social media and why learners should be concerned.	Watch video	https://www.cdse.edu/Training/Security-Training-Videos/Cybersecurity/Social-Media/
SOCIAL ENGINEERING	Team's ability to identify cyber-risk	The course introduces learners to cyber-risk management for developing abilities to assess vulnerabilities and handle intrusions.	Read and watch video	https://fedvte.usalearning.gov/publiccourses/fcrmframe.php
DENIAL OF SERVICE	Employees' security behaviour consistent with the organisation's information security policy	The purpose of the course is to influence behaviour by focusing on actions that authorised users can engage to mitigate threats and vulnerabilities to information systems.	Read and watch video	https://securityawareness.usalearning.gov/insiderthreatprgm/index.htm
MALICIOUS INSIDER	Lack of adherence to security procedures	In order to ensure accountability, employees must be knowleageable about an organisation's procedures. Confidential information can be kept safe.	Read and do activities	Step 1: Sign Up: greatlearning (mygreatlearning.com) Step 2: Log In to Course: https://olympus.mygreatlearning.com/courses/12628/pages/security-goals-and-its-implementations-confidentiality?module_item_id=926343
STOLEN CREDENTIALS/ UNAUTHORISED ACCESS	Create awareness through desktop images, screensavers, user awareness mails	Cybersecurity posters are available for download and promoting security awareness in the workplace.	Read content from posters	https://www.cdse.edu/Training/Security-Posters/Cybersecurity/

6 IDENTIFICATION OF WORK ROLES IN WATER SECTOR AND GAP ANALYSIS

The water sector has attempted to bridge the gap between operating and information technologies by overlapping these systems to reduce maintenance costs and optimise the control and monitoring systems. The potential for cyberthreats has increased due to the overlapping of these systems (Wei et al., 2010; Skiba, 2020). To help address these issues, the National Cybersecurity Policy Framework (NCPF) was released by the South African government in 2015. However, the framework does not outline the cybersecurity practitioners' work roles for the water sector of South Africa (State Security Agency, 2015). Currently, there is no clear definition of the required work roles of cybersecurity practitioners in the water sector of South Africa.

The aim of this research was to create a framework that will define cybersecurity practitioners' work roles for the South African water sector within the National Institute of Standards and Technology (NIST), National Initiative for Cybersecurity Education (NICE), Cybersecurity Workforce Framework (CWF) (Petersen et al., 2020) and other international and national best practice guidelines and frameworks. To develop the framework, the water sector organisational structure was defined from literature and cybersecurity considerations, and based on the defined considerations, cybersecurity work roles were defined and any gaps identified were closed.

This research is vital to the water sector because it will provide water quality and quantity assurance to South Africa's diverse domestic and strategic water users by defining the required cybersecurity work roles and thereby decrease the water sector's potential for cyberthreats.

6.1 Methodology

This study adopted the qualitative content analysis methodology using secondary data identified from literature. This methodology was utilised because it ensures that the original data is preserved, the data is analysed systematically rather than selectively and qualitative data can be analysed and frameworks constructed (Lancaster, 2005; Sekaran & Bougie, 2016). The methodology followed was adapted from Von Solms and Marnewick (2018) to define the work roles of cybersecurity practitioners in the water sector of South Africa:

1. A literature review was conducted to define the South African water sector organisational structure and identify frameworks and guidelines to define the

cybersecurity considerations and cybersecurity practitioner work roles for the South African water sector.

2. The cybersecurity considerations for the water sector were defined by using ISO 27002 as the baseline data source. Verification and validation of the considerations extracted from ISO 27002 were performed by using the other data sources identified.
3. The work roles of cybersecurity practitioners were defined by listing all the cybersecurity work roles and their definitions from the NIST NICE CWF. A meaning unit was defined; in this case, defining the meaning unit refers to condensing the work role definition. The meaning unit was then categorised and coded. The code was used to match the work role to a specific cybersecurity consideration. Validation and verification were carried out by using the Skills Framework for the Information Age (SFIA).
4. The results from the data analysis process were interpreted to construct a framework to address the research aim.

6.2 Related literature

Water sector organisational structure

To start to address the concerns regarding the threat to water quantity and quality, the South African water sector organisational structure must be understood. Legislation and policies are developed at ministerial level (Beck et al., 2016). Departmental level is responsible for governance related to policies and legislation. This level also ensures and enforces compliance (Ruiters & Matji, 2015). National and regional levels are responsible for the development and management of all procedures (GreenCape, 2014). Local level is responsible to ensure that policies and procedures are carried out within their jurisdictions. Plant level carries out and implements all procedures and policies. This level will also monitor, control and report any anomalies which may adversely impact plant operations (GreenCape, 2014; Ruiters & Matji, 2015; Beck et al., 2016).

The structure of the South African water sector can be seen in Figure 36 below. The figure indicates the governance structure as well as highlights its importance in relation to the cybersecurity domains.

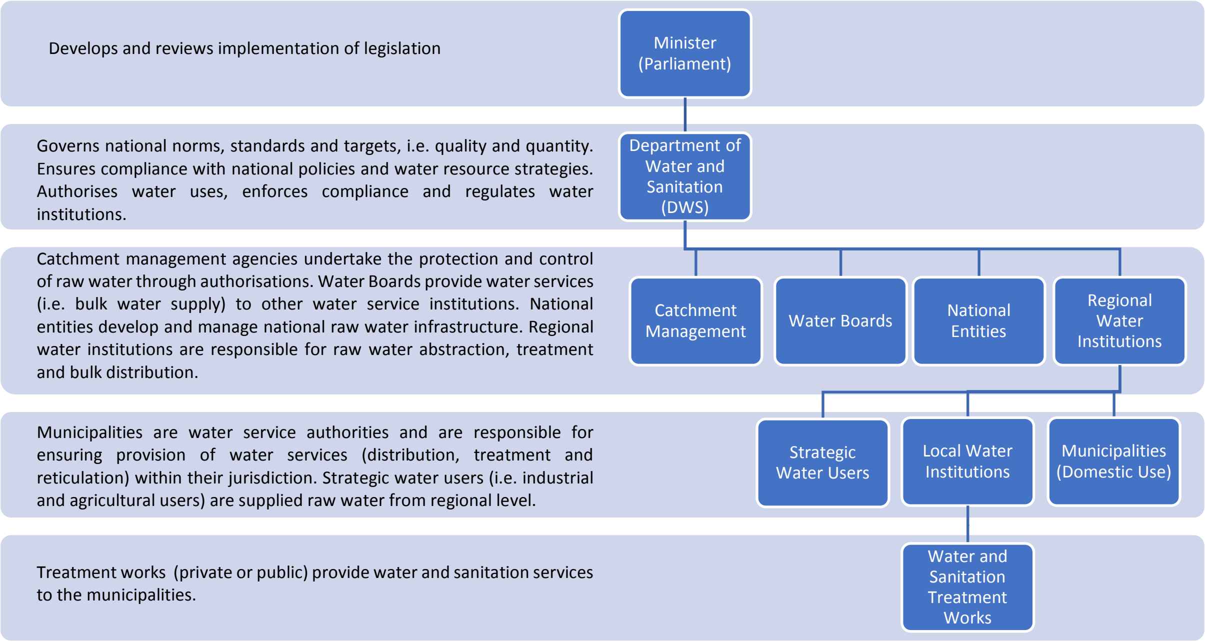

Develops and reviews implementation of legislation
Minister (Parliament)
Governs national norms, standards and targets, i.e. quality and quantity. Ensures compliance with national policies and water resource strategies. Authorises water uses, enforces compliance and regulates water institutions.
Department of Water and Sanitation (DWS)
Catchment management agencies undertake the protection and control of raw water through authorisations. Water Boards provide water services (i.e. bulk water supply) to other water service institutions. National entities develop and manage national raw water infrastructure. Regional water institutions are responsible for raw water abstraction, treatment and bulk distribution.
Catchment Management
Water Boards
National Entities
Regional Water Institutions
Municipalities are water service authorities and are responsible for ensuring provision of water services (distribution, treatment and reticulation) within their jurisdiction. Strategic water users (i.e. industrial and agricultural users) are supplied raw water from regional level.
Strategic Water Users
Local Water Institutions
Municipalities (Domestic Use)
Treatment works (private or public) provide water and sanitation services to the municipalities.
Water and Sanitation Treatment Works

Figure 36: Governance, roles and functions of organs of state in the water sector in South Africa (GreenCape, 2014; Ruiters & Matji, 2015; Beck et al., 2016)

Each hierarchy in the roles and responsibilities of the water sector is defined as follows:

- Ministerial level: Develops, reviews and implements legislation.
- Departmental level: Governs national norms, standards and targets. Ensures compliance with policies and strategies. Authorisation and enforcement of compliance are governed at this level.
- National and regional levels: Develop and manage procedures.
- Local level: Municipalities are responsible for ensuring that policies and procedures are carried out within their jurisdiction.
- Plant level: Water service providers (can be public, private or mixed entities) carry out all legislation, policies and procedure to ensure detection, mitigation and prevention of cyberattacks.

The entire hierarchy of the water sector must be taken into account to fulfil the numerous work roles required for a successful cybersecurity programme to establish a sustainable cybersecurity structure within the water sector (Panguluri et al., 2011). Figure 36 indicates the hierarchy of the water sector and the roles and responsibilities at each level. Legislation and overall governance are developed at the highest level, and enforced and conducted further down the hierarchy. The operating level will be responsible for operating, monitoring and controlling cybersecurity measures.

The water sector hierarchy can be applied to the roles and responsibilities related to cybersecurity. Cybersecurity policies and governance are developed at the highest levels as per the organisational structure. Compliance will be enforced by the departmental level and municipalities will be responsible to supply the correct quality and quantity of water to its users by ensuring that cybersecurity measures are in place. Catchment agencies, water boards and national entities level must ensure a cybersecure environment for the safe supply of water. Water and wastewater treatment plant level needs to monitor and report any anomalies related to cybersecurity and any adverse impacts it may have on the plant operation and the water quantity and qualities.

Frameworks and guidelines to define the cybersecurity considerations for the water sector

Internationally, a variety of cybersecurity frameworks, guidelines and standards have been produced or are in the process of being developed (Panguluri et al., 2011; Germano, 2019). ISO 27002 of the International Organization for Standardization (2013) has been adopted by the South African Bureau of Standards (SABS). It specifies an organisation's minimum information security criteria. Other data sources identified are the "Guide to Industrial Control Systems (ICS) Security" (Stouffer & Candell, 2015), "15 cybersecurity fundamentals for water and wastewater utilities: Best practices to reduce exploitable weaknesses and attacks" (Water Information Sharing and Analysis Center, 2019), "Water sector cybersecurity risk management guidance" of the American Water Works Association (AWWA) (Yost, 2019) and the "Roadmap to secure control systems in the water sector" (Water Sector Coordinating Council Cybersecurity Working Group, 2008). The documents mentioned can be used to define the cybersecurity considerations for the water sector of South Africa.

Gaps identified from literature indicate that the cybersecurity industry is relatively new and many of its standards and guidelines are still being developed (Panguluri et al., 2011). Not all the cybersecurity requirements for the water sector have been identified, but have rather been developed based on known threats and vulnerabilities (Water Sector Coordinating Council Cybersecurity Working Group, 2008; Germano, 2019; Yost, 2019). Literature also indicates that methods of physical security, access and authentication, software enhancements and privacy enhancements are all cybersecurity components which are lacking. Another gap identified is the requirements for improving the security between the business and ICS network as well as intrusion detection (Panguluri et al., 2011; Clark et al., 2016; Germano, 2019).

Frameworks and guidelines to define the work roles of cybersecurity practitioners

The Skills Framework for the Information Age (SFIA) is a model for characterising and managing skills and competencies for information and communication technologies (ICT) and cybersecurity professionals. The model assists with understanding IT skills in general and it contains security-related skills (Furnell, 2021). SFIA describes the abilities and competencies required by professionals in positions involving ICT and cybersecurity (SFIA Foundation, 2018).

According to Caulkins et al. (2019), the demand for cybersecurity practitioners is growing. Competent cybersecurity practitioners are hard to come by in all industries and companies (Campbell et al., 2015). The NIST NICE CWF acts as a guiding principle for the development of a unified cybersecurity workforce. It details the requirements for workforce identification, and standardises development of work role descriptions, qualification requirements and training requirements for the development of a capable and ready workforce (Dawson et al., 2019; Schmeelk & Dragos, 2020). The NIST NICE CWF was released in order to develop a process for determining specific cybersecurity work roles (Campbell et al., 2015). It was used as the baseline data source for this study.

Gaps identified show that the educational programmes at various institutes are not aligned with the NIST NICE CWF, especially in the *analyse* and *investigate* categories (Caulkins et al., 2019; Saharinen et al., 2020). Another gap is that the NIST NICE CWF focuses on the technical skills required for the cybersecurity workforce; however, research (Campbell et al., 2015; Caulkins et al., 2019) indicates that non-technical skills are just as important as the technical kind. Based on current professionals within the industry, the work roles framework that was identified may not be implementable due to the lack of educational programmes available, grasp of non-technical skills and the availability of experienced individuals.

6.3 Water sector cybersecurity considerations

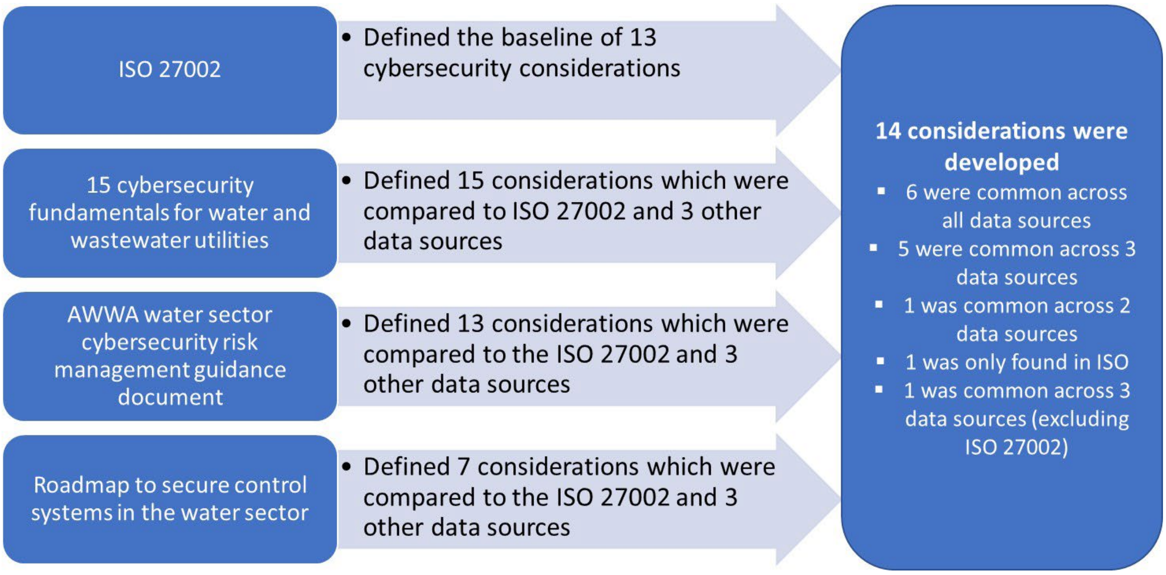
To establish the appropriate work roles for cybersecurity practitioners in the water sector, the cybersecurity considerations for the South African water sector were firstly determined. The considerations were collected from four different data sources:

1. ISO 27002 (International Organization for Standardization, 2013; Diamantopoulou et al., 2020).
2. Water Information Sharing and Analysis Center's 15 cyber security fundamentals for water and wastewater utilities

3. AWWA’s water sector cybersecurity risk management guidance document (Yost, 2019)
4. The roadmap to secure control systems in the water sector (Water Sector Coordinating Council Cybersecurity Working Group, 2008)

The data collected was combined and examined to create a comprehensive set of cybersecurity considerations for the water sector in South Africa.

Firstly, ISO 27002 was used to list and define the baseline of cybersecurity considerations. Secondly, these considerations were verified against the three other data sources by performing latent and manifest analysis on the definitions of the considerations. A total of 14 considerations were defined, summarised in Figure 37.



ISO 27002
• Defined the baseline of 13 cybersecurity considerations
15 cybersecurity fundamentals for water and wastewater utilities
• Defined 15 considerations which were compared to ISO 27002 and 3 other data sources
AWWA water sector cybersecurity risk management guidance document
• Defined 13 considerations which were compared to the ISO 27002 and 3 other data sources
Roadmap to secure control systems in the water sector
• Defined 7 considerations which were compared to the ISO 27002 and 3 other data sources
14 considerations were developed
▪ 6 were common across all data sources
▪ 5 were common across 3 data sources
▪ 1 was common across 2 data sources
▪ 1 was only found in ISO
▪ 1 was common across 3 data sources (excluding ISO 27002)

Figure 37: Data analysis process flow to define the water sector cybersecurity considerations of South Africa

Table 23 indicates the comparable considerations across the different data sources. A total of 14 considerations were developed. An overall title for the requirement was created based on its description. The title of the consideration also acts as a key word to link the specific consideration to the data source(s) from which it was derived. The work roles of cybersecurity practitioners in the water sector of South Africa were based on these considerations.

Table 23: Step 3 – Cybersecurity considerations for the water sector

No.	Consideration	Description	DATA SOURCE COMPARISONS			
			ISO 27002	15 cyber security fundamentals for the water and wastewater utilities	AWWA's Water sector cybersecurity risk management guidance document	Roadmap to secure control systems in the water sector
1	Asset management	All assets, including but not limited to data, processes, people and supporting infrastructure, such as all components on IT and OT networks, in the field, third-party and legacy equipment, are identified. This is part of the strategy and plan for managing cybersecurity risks. This is crucial because the organisation needs to know what to protect.	✓	✓	✓	✓
2	Risk assessment & management	A risk assessment's purpose is to identify and prioritise risk based on the likelihood of a threat or vulnerability having a negative impact on a business. The establishment of a cybersupply chain risk management plan, which involves setting cybersecurity considerations for suppliers, communicating those considerations and ensuring that they are met, will be among the activities. Additional activities are the establishment of a risk management strategy for the organisation as well as carrying out vulnerability assessments.		✓	✓	✓
3	Governance	It is vital to design and implement clear and effective cybersecurity governance, policies and procedures for all IT and OT systems. Policies and procedures should clearly describe a company's cybersecurity obligations. Security system administration and executive control are linked to establishing organisational boundaries and a framework of security rules, processes and systems to manage the organisation's confidentiality, integrity and availability. It is also crucial for the development of ICS security programmes, since they must reflect changes in governance, norms and processes, as well as technological advancements.	✓	✓	✓	
4	Human resource security & cybersecurity awareness	This guarantees that employees and contractors are aware of their obligations and can do the tasks assigned to them. This area deals with raising security awareness among the organisation's employees, clients and service providers. An adversary with physical or privileged access can swiftly undermine strong protective cybersecurity policies and system architecture. The greater their awareness of the situation, the better. Leadership support, as well as training and awareness programmes, are essential for establishing a cybersecurity culture. As cyberattackers migrate from hacking computers to targeting people, not only can vulnerabilities and dangers go unreported if employees are not involved in cybersecurity, but they can also become accidental insider threats or conduits via which assaults are carried out.	✓	✓	✓	✓

No.	Consideration	Description	DATA SOURCE COMPARISONS			
			ISO 27002	15 cyber security fundamentals for the water and wastewater utilities	AWWA's Water sector cybersecurity risk management guidance document	Roadmap to secure control systems in the water sector
5	Access control	This category is concerned with ensuring that only authorised individuals have access to the organisation's computing resources. Access control refers to restricting access to a control system to only those who are authorised to use it. Roles and duties must be clearly specified before access and permissions can be restricted.	✓	✓	✓	✓
6	Physical & environmental security	Physical access should be limited and restricted to just authorised personnel who need to interface with the hardware, as hackers can swiftly gain access to sensitive data and systems via physical equipment. Physical access should be restricted to IT and ICS settings, as well as communications equipment and assets in remote locations.	✓	✓	✓	
7	Operations security	Establishing a security operations centre (SOC) for continuous threat detection and monitoring is critical. Collecting, correlating and analysing network, host and application security events will be one of its primary functions. It also focuses on fine-tuning operational procedures and workflows to improve an organisation's security.	✓	✓	✓	
8	Business continuity, incidents, emergencies and disaster recovery planning	An emergency response plan, a continuity of operations strategy and/or a disaster recovery/business continuity plan, among other disaster recovery and business continuity measures, must be designed, maintained and monitored. Organisational reaction abilities should be tested and developed, and tactics should be tested and changed, through exercises. Business continuity planning is a methodical approach to prepare for and limit the risk and impact of system and operational failure in a company. It ensures that the control system continues to function even if there are errors and that service interruptions are rectified quickly.	✓	✓	✓	
9	Securing the supply chain	Improved security protocols are essential not only internally, but also in all third-party relationships. Risk assessments should encompass supply chains, such as vendors, contractors and consultants. For all supply chain relationships, governance, policies and procedures must be defined and supply chain CSA needs to be reinforced. The supply chain relationships must be subjected to regular risk assessments, threat detections and vulnerability evaluations.	✓	✓		✓
10	Cryptography, design and implementation	Utilities use design elements to protect critical assets from several threats. Integrating historical systems with new modern systems that include or increase security elements is crucial as technology advances regularly and at a rapid pace. New and	✓	✓	✓	✓

No.	Consideration	Description	DATA SOURCE COMPARISONS			
			ISO 27002	15 cyber security fundamentals for the water and wastewater utilities	AWWA's Water sector cybersecurity risk management guidance document	Roadmap to secure control systems in the water sector
	of improved security systems	improved systems that will increase productivity and dependability while also incorporating security features will be required.				
11	Participate in partnership and outreach for information sharing and collaboration	Other critical infrastructure sectors are at risk from the same cyberthreats that endanger water and wastewater utilities. Participating in cybersecurity and resilience groups helps members of the community to learn from one another and share their knowledge and experiences. To increase the sector's ability to plan for and respond to cyberdisasters, collaborative partnerships will pool resources and capabilities from utilities, associations, vendors, communities, government agencies and others. ICS security demands are handled and anticipated from all angles by combining the skills and viewpoints of all sectors of the industry.	✓	✓	✓	✓
12	Systems acquisition, development and maintenance	To achieve acceptable security levels, organisations attempt to control risk. Physical and logical network segmentation, traffic-restricting devices and software, control system design and configuration document protection, encrypted communications, stringent processes and physical security are all required to achieve this. Vulnerability management is a process that never ends. Its purpose is to protect servers and workstations from cyberattacks by defining best practices for lowering the likelihood of unwanted server access and maintaining server and system attributes.	✓	✓	✓	✓
13	Communication security	Given that employees rely on smart devices to complete their work, it is vital that safe and secure device usage be included in training and awareness initiatives.	✓			✓
14	Compliance	This is required to avoid breaking any information security-related legal, legislative, regulatory, or commercial obligations or security standards.	✓			

6.4 Defining the work roles of cybersecurity practitioners

Data was collected from the NIST NICE CWF and analysed to define the work roles of cybersecurity practitioners in the water sector based on cybersecurity considerations. SFIA was used for verification and validation. Figure 38 shows the steps that were taken to develop a comprehensive set of cybersecurity practitioner work roles for the water sector in South Africa. Steps 1-3 relate to data analysis to define the work roles of cybersecurity practitioners in the water sector, and steps 4-5 relate to the validation and verification.

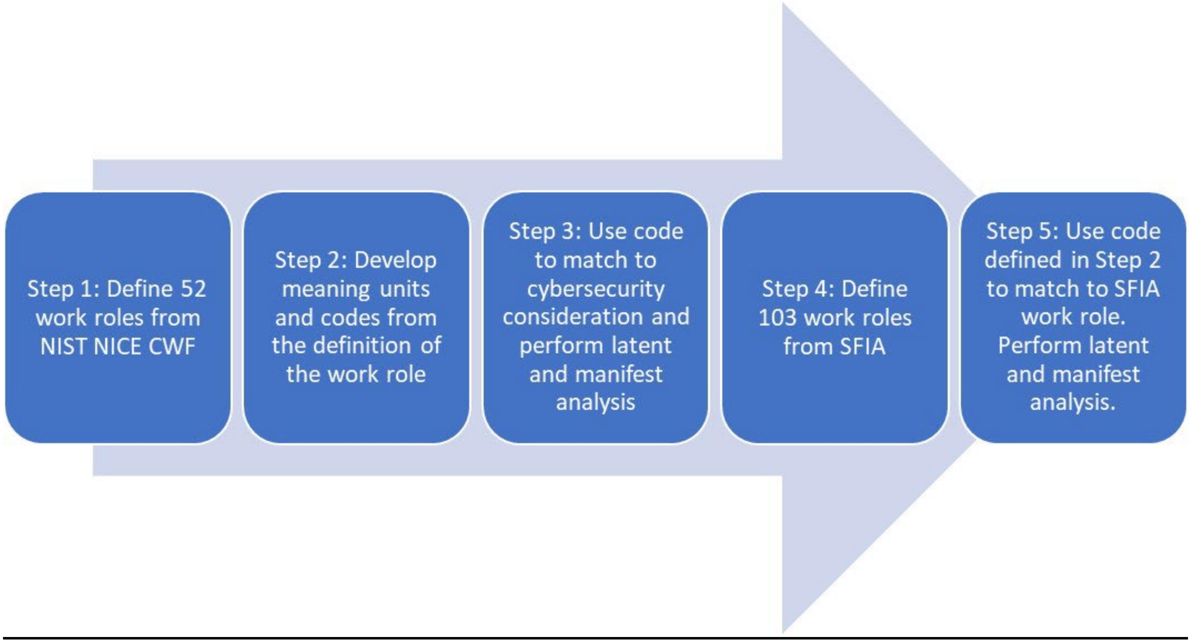

Step 1: Define 52 work roles from NIST NICE CWF
Step 2: Develop meaning units and codes from the definition of the work role
Step 3: Use code to match to cybersecurity consideration and perform latent and manifest analysis
Step 4: Define 103 work roles from SFIA
Step 5: Use code defined in Step 2 to match to SFIA work role. Perform latent and manifest analysis.

Figure 38: Steps taken to develop a comprehensive set of cybersecurity practitioner work roles for the water sector in South Africa

Data analysis

This section shows the content analysis process which was conducted on the cybersecurity work roles by using the NIST NICE CWF as the baseline data source. The following steps, as per the process flow diagram in Figure 38, were taken to develop the results found in Table 24 below.

Step 1: Categories and work roles as defined by NIST NICE CWF (Newhouse et al., 2017; Petersen et al., 2020) are listed and numbered in Table 24, columns 1, 2 and 3.

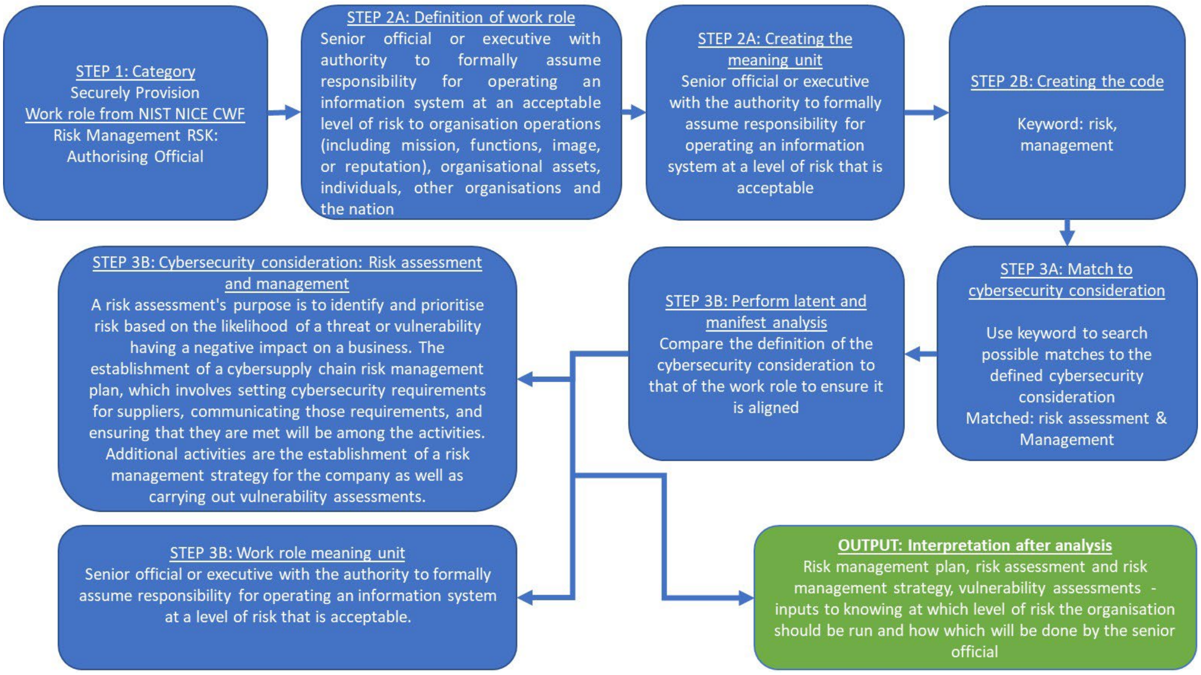
Step 2a: The definition of each work role from NIST NICE CWF was used to develop the meaning unit which can be seen in column 4, Table 24. The meaning unit was developed by condensing the definition of each work role from NIST NICE CWF.

Step 2b: The meaning unit was coded. Keywords from the meaning unit were taken to create a unique code. It was important that the code not be duplicated and confused with another code. To circumvent this, multiple keywords were used in conjunction with each other to code for a specific meaning unit. This can be seen in column 5, Table 24.

Step 3a: The newly created code was used to match the work role to a specific water sector cybersecurity consideration which was defined in Table 24.

Step 3b: Latent and manifest analysis was then performed to ensure that the correct work role was matched to the correct cybersecurity consideration. This can be seen in column 6, Table 24.

Each step is explained by applying the data analysis process to one of the work roles. The example is in reference to item #1 *Risk Management (RSK): Authorising Official*, in Table 24. Figure 39 shows the process which was followed as well as how each step was applied to ultimately match the NIST NICE CWF work role to a cybersecurity consideration.



STEP 1: Category
Securely Provision
Work role from NIST NICE CWF
Risk Management RSK: Authorising Official

STEP 2A: Definition of work role
Senior official or executive with authority to formally assume responsibility for operating an information system at an acceptable level of risk to organisation operations (including mission, functions, image, or reputation), organisational assets, individuals, other organisations and the nation

STEP 2A: Creating the meaning unit
Senior official or executive with the authority to formally assume responsibility for operating an information system at a level of risk that is acceptable

STEP 2B: Creating the code
Keyword: risk, management

STEP 3A: Match to cybersecurity consideration
Use keyword to search possible matches to the defined cybersecurity consideration
Matched: risk assessment & Management

STEP 3B: Perform latent and manifest analysis
Compare the definition of the cybersecurity consideration to that of the work role to ensure it is aligned

STEP 3B: Cybersecurity consideration: Risk assessment and management
A risk assessment's purpose is to identify and prioritise risk based on the likelihood of a threat or vulnerability having a negative impact on a business. The establishment of a cybersupply chain risk management plan, which involves setting cybersecurity requirements for suppliers, communicating those requirements, and ensuring that they are met will be among the activities. Additional activities are the establishment of a risk management strategy for the company as well as carrying out vulnerability assessments.

STEP 3B: Work role meaning unit
Senior official or executive with the authority to formally assume responsibility for operating an information system at a level of risk that is acceptable.

OUTPUT: Interpretation after analysis
Risk management plan, risk assessment and risk management strategy, vulnerability assessments - inputs to knowing at which level of risk the organisation should be run and how which will be done by the senior official

Figure 39: Example of how the data analysis process was followed for steps 1-3 based on item #1 from Table 24

Figure 39 depicts steps 1 to 3 of how the work role, *Risk Management: Authorising Official,* was matched to a specific cybersecurity consideration.

Step 1: The category and work role for the *Risk Management: Authorising Official* were stated.

Step 2a: The definition of *Risk Management: Authorising Official* as per the NIST NICE CWF was stated and then condensed to form the meaning unit.

Step 2b: Specific keywords were used from the meaning unit for coding. The keywords “risk” and “management” were selected.

Step 3a: The code from 2b was used to search through the cybersecurity considerations defined in Table 24 and matched with the consideration “Risk assessment and management”.

Step 3b: Latent and manifest analysis was performed by stating the definition of the consideration “Risk assessment and management” as well as the definition of the work role *Risk Management: Authorising Official*. The two definitions were compared to each other and interpreted. The interpretation revealed that the risk management plan, risk assessment, risk management strategy and vulnerability assessments are required as inputs to ensure that the risk, risk consequences, as well as risk ratings are understood and known. The *Risk Management: Authorising Official* is required to know the risks, risk consequences, as well as risk ratings in order to take responsibility for operating the organisation effectively and at an acceptable risk level.

The results of steps 1 to 3 led to the conclusion that the job title *Risk Management: Authorising Official* corresponds to the cybersecurity consideration “Risk assessment and management”, shown in green in Table 24.

The process as depicted in Figure 39 was repeated for all 52 work roles. Once the process was completed, 37 work roles matched to a specific cybersecurity consideration. Four work roles, namely numbers 8, 37, 40 and 41 from Table 24, were deemed as important but did not match any cybersecurity consideration. These four work roles, along with the 37 already matched to cybersecurity considerations, were applied to steps 5 and 6 to establish if they should be included as part of the final framework. Two cybersecurity considerations, namely numbers 42 and 43 from Table 24, did not match any of the work roles of the NIST NICE CWF. These considerations were applied to steps 5 and 6 to determine if they should be added to the overall framework and deemed as a gap.

Table 24: Content analysis results of work roles in relation to cybersecurity considerations for the water sector

1: No.	2: Category	3: Work roles from NIST NICE CWF	4: Meaning unit	5: Code	6: Cybersecurity considerations for the South African water sector
1	Securely Provision	Risk Management (RSK): Authorising Official	Senior official or executive with the authority to formally assume responsibility for operating an information system at a level of risk that is acceptable.	risk management	Risk assessment & management
2	Securely Provision	Risk Management (RSK): Security Control Assessor	Determines the overall efficacy of management, operational and technical security controls and control upgrades applied within an IT system.	independent assessments, audit	Risk assessment & management
3	Securely Provision	Software Development: Software Developer	Develops, builds, manages and writes/codes new computer applications, software, or specialised utility programs.	software development	Cryptography, design and implementation of improved security systems
4	Securely Provision	Software Development: Secure Software Assessor	Provides actionable results after analysing the security of new or current computer applications, software, or specialised utility programs.	assessments, software	Cryptography, design and implementation of improved security systems
5	Securely Provision	Systems Architecture: Security Architect	Ensures that all aspects of enterprise architecture and the resulting systems supporting those missions and business processes adequately address the stakeholder security requirements necessary to protect the organisation.	security, architecture	Cryptography, design and implementation of improved security systems
6	Securely Provision	Technology R&D: Research and Development Specialist	Conducts software and systems engineering and software systems research to build new capabilities while assuring complete cybersecurity integration. Conducts in-depth technological study to assess cyberspace system vulnerabilities.	research, new technology, innovation	Participate in partnership and outreach for information sharing and collaboration
7	Securely Provision	Systems Development: Systems Developer	Throughout the systems development life cycle, designs, develops, tests and evaluates information systems.	systems development, design, test	Cryptography, design and implementation of improved security systems
8	Securely Provision	Test & Evaluation: System Test & Evaluation Specialist	Plans, prepares and conducts system tests to compare results to specifications and requirements and to analyse and report test results.	test	
9	Securely Provision	Systems Development: Information Systems Security Developer	Throughout the systems development life cycle, designs, develops, tests and analyses information system security.	systems development, security	Cryptography, design and implementation of improved security systems
10	Operate and Maintain	Data Administration: Database Administrator	Administers databases and/or data management systems that allow data to be securely stored, queried and used.	data administration	Asset management
11	Operate and Maintain	Data Administration: Data Analyst	Examines data from a variety of sources to provide security and privacy insight. Custom algorithms and workflow procedures used for modelling, data mining and research are designed and implemented.	analysis	Asset management
12	Operate and Maintain	Knowledge Management: Knowledge Manager	Managing and administering processes and systems that enable the company to identify, document and access intellectual capital and information content.	knowledge, management	Asset management
13	Operate and Maintain	Systems Analysis: Systems Security Analyst	Analysis and development of system security integration, testing, operations and maintenance.	integration, security, systems	Access control
14	Oversee and Govern	Legal Advice and Advocacy: Cyber Legal Advisor	Provides legal counsel and recommendations on a variety of cyber-related issues.	legal	Compliance
15	Oversee and Govern	Legal Advice and Advocacy: Privacy Officer/Privacy Compliance Manager	Develops and manages the privacy compliance programme and its employees, assisting privacy and security leaders and their teams with privacy compliance, governance/policy and incident response.	legal	Compliance

1: No.	2: Category	3: Work roles from NIST NICE CWF	4: Meaning unit	5: Code	6: Cybersecurity considerations for the South African water sector
16	Oversee and Govern	Training, Education and Awareness: Cyber Instructional Curriculum Developer	Based on instructional needs, develops, arranges, coordinates and evaluates cybertraining/education courses, methodologies and procedures.	learn, train, awareness, training	Human resource security & cybersecurity awareness
17	Oversee and Govern	Training, Education and Awareness: Cyber Instructor	Develops and performs staff training or education in the cyber-realm.	training, trainer	Human resource security & cybersecurity awareness
18	Oversee and Govern	Cyber Security Management: Information Systems Security Manager	In charge of cybersecurity of a program, organisation, system, or enclave.	management, IT, security	Governance
19	Oversee and Govern	Cyber Security Management: Communications Security Manager	Individual who manages the communications security resources of an organisation or key custodian of a crypto key management system.	mobile devices, communication, security	Communication security
20	Oversee and Govern	Strategic Planning and Policy: Cyber Workforce Developer and Manager	Develops cyberspace workforce plans, strategies and guidelines to support cyberspace workforce human resources, personnel, training and education needs, as well as to handle changes in cyberspace policy, doctrine, material, force structure and education and training needs.	resources, personnel training, development	Human resource security & cybersecurity awareness
21	Oversee and Govern	Strategic Planning and Policy: Cyber Policy and Strategy Planner	To support and align with organisational cybersecurity efforts and regulatory compliance, develops and maintains cybersecurity plans, strategy and policy.	strategic, plan, policies	Governance
22	Oversee and Govern	Executive Cyber Leadership: Executive Cyber Leadership	Establishes vision and direction for an organisation's cyber and cyber-related resources and operations by executing decision-making authority.	oversight, authority, security	Governance
23	Oversee and Govern	Program/Project Management and Acquisition: IT Program Auditor	Conducts assessments of an IT program or its constituent components to evaluate if they meet stated requirements.	audit, check, program management	Governance
24	Protect and Defend	Cyber Defence Analysis: Cyber Defence Analyst	Analyses events that occur within their environments using data acquired from a range of cyberdefence instruments for the objective of reducing risks.	security, analysis, threat detection	Operations security
25	Protect and Defend	Cyber Defence Infrastructure Support: Cyber Defence Infrastructure Support Specialist	The infrastructure hardware and software is tested, implemented, deployed, maintained and administered.	specialist	Participate in partnership and outreach for information sharing and collaboration
26	Protect and Defend	Incident Response: Cyber Defence Incident Responder	Within the network environment or enclave, investigates, analyses and responds to cyberevents.	incident	Business continuity, incidents, emergencies and disaster recovery planning
27	Protect and Defend	Vulnerability Assessment and Management: Vulnerability Assessment Analyst	Assesses systems and networks and determines where they depart from permitted configurations, enclave policy, or local policy. Measures the efficacy of a defence-in-depth architecture against known flaws.	vulnerability assessment, events	Systems acquisition, development and maintenance
28	Analyse	Warning/Threat Analysis: Threat/Warning Analyst	Creates cyberindicators to keep track of the state of the extremely dynamic working environment. Cyberthreat assessments are collected, processed, analysed and disseminated.	risks, mitigations, warnings	Systems acquisition, development and maintenance
29	Analyse	Exploitation Analysis: Exploitation Analyst	Collaborates to identify gaps in access and collection that can be addressed through cybercollection and preparation actions.	exploitation, dangers, security	Systems acquisition, development and maintenance
30	Analyse	All-Source Analysis: All-Source Analyst	Analyses data from different sources to conduct environmental preparation, respond to information requests and submit intelligence collection and production requirements in support of planning and operations.	data, analysis, multiple sources	Systems acquisition, development and maintenance
31	Analyse	All-Source Analysis: Mission Assessment Specialist	Develops performance measures and assessment plans as needed for cyberincidents, conducts strategic and operational efficacy assessments. Determines whether systems function as intended and contributes to operational effectiveness.	performance, measure	Systems acquisition, development and maintenance

1: No.	2: Category	3: Work roles from NIST NICE CWF	4: Meaning unit	5: Code	6: Cybersecurity considerations for the South African water sector
32	Analyse	Targets: Target Developer	Performs target system analysis, creates and maintains electronic target folders with information from environment preparation and/or internal and external intelligence sources. Coordinates with partner target operations and intelligence agencies.	Targets, requirements	Systems acquisition, development and maintenance
33	Analyse	Targets: Target Network Analyst	Conducts advanced analysis of collected and open-source data to maintain target continuity, profile targets and their behaviours and develop strategies to learn more about them. Based on information collected, determines how targets communicate, move, operate and live.	Network, data, security, analysis	Systems acquisition, development and maintenance
34	Analyse	Language Analysis: Multi-Disciplined Language Analyst	Processes, analyses and disseminates intelligence information generated from language, voice and graphic material, combining language and culture experience with threat and technological knowledge. To assist cyberaction execution and ensure crucial knowledge sharing, creates and maintains language-specific databases and working aids.	code, language	Systems acquisition, development and maintenance
35	Collect and Operate	Cyber Operational Planning: Cyber Intel Planner	Develops precise intelligence plans to meet the needs of cyberoperations. Collaborates with cyberoperations planners to determine, validate and levy gathering and analysis requirements. Participates in cyberaction targeting, validation, synchronisation and execution.	plan, policies, investigate, crime, cyber	Business continuity, incidents, emergencies and disaster recovery planning
36	Collect and Operate	Cyber Operational Planning: Cyber Ops Planner	Through collaboration with other planners, operators and/or analysts, develops detailed plans for the conduct or support of the appropriate range of cyberactivities.	plan, operations, policies	Business continuity, incidents, emergencies and disaster recovery planning
37	Collect and Operate	Cyber Operational Planning: Partner Integration Planner	Collaboration between cyberoperations partners across organisational or country lines is promoted. Provides direction, tools and collaboration to help partner cyberteams to integrate by developing best practices and facilitating organisational support.	integration, across borders, collaboration	Participate in partnership and outreach for information sharing and collaboration
38	Collect and Operate	Cyber Operations: Cyber Operator	Collects, processes and/or geolocates information from systems to exploit, locate and/or track targets of interest. Performs network navigation, tactical forensic analysis and on-net activities as required.	crime, operator, investigate	Operations security
39	Investigate	Cyber Investigation: Cyber Crime Investigator	Using regulated and recorded analytical and investigative processes, locates, acquires, examines and maintains evidence.	evidence, collection	
40	Investigate	Digital Forensics: Law Enforcement/Counterintelligence Forensics Analyst	Conducts in-depth investigations into computer-related crimes and logs associated with cyberintrusion occurrences, to establish documentary or physical proof.	crime, criminal, security, threats	
41	Investigate	Digital Forensics: Cyber Defence Forensics Analyst	Analyses digital evidence and examines computer security occurrences to gather knowledge that can be used to help mitigate network vulnerabilities.	crime, analyses, investigate	
42					Physical & environmental security
43					Securing the supply chain

The NIST NICE CWF listed 52 work roles. The 9 work roles which have not been added to Table 24 were not specific to the cybersecurity discipline, i.e. work roles related to general project management and customer service. It is assumed that these roles would already be filled as part of the IT service of an organisation and are not specific to cybersecurity.

In Table 24 gaps have been identified, highlighted in orange. Two types of gaps have been identified and are indicated below:

Gap 1: Shortcomings in the water sector cybersecurity considerations

- Item 8: Test & Evaluation: System Test & Evaluation Specialist
- Item 39: Cyber Investigation: Cyber Crime Investigator
- Item 40: Digital Forensics: Law Enforcement/Counterintelligence Forensics Analyst
- Item 41: Digital Forensics: Cyber Defence Forensics Analyst

Gap 2: Shortcomings in defined work roles in the NIST NICE CWF

- Item 42: Physical and environmental security
- Item 43: Securing the supply chain

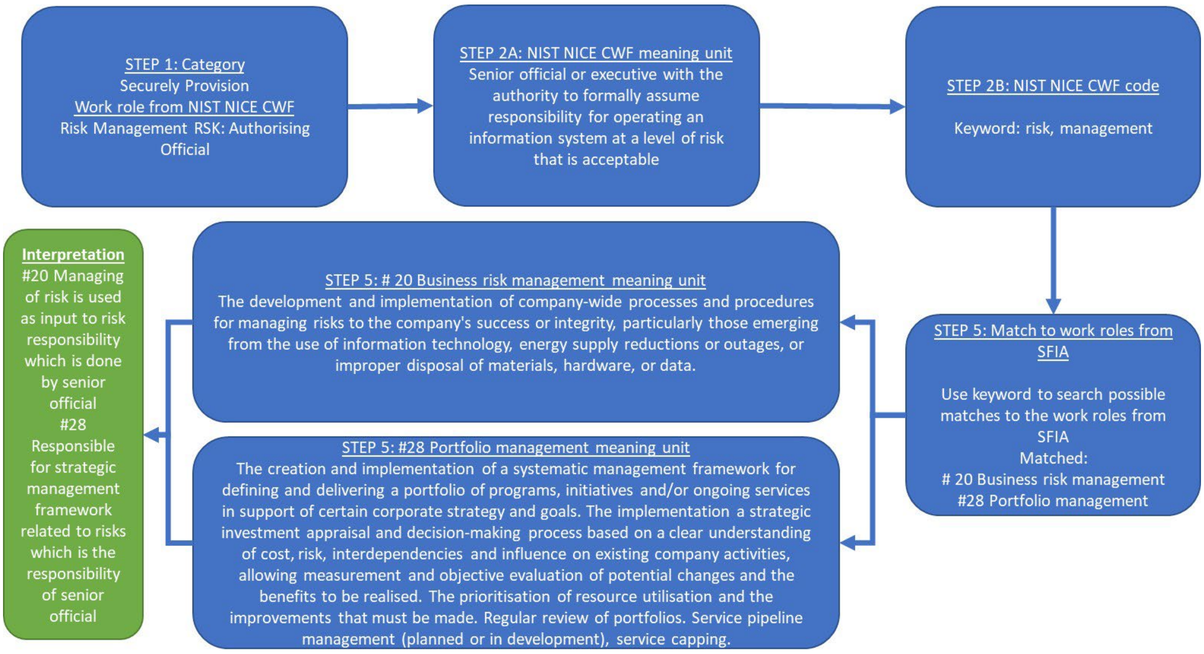
Verification and validation

Next, verification and validation of the NIST NICE CWF work roles were performed using the work roles or job descriptions as defined by SFIA. Refer to Figure 40, steps 4 and 5 of the process flow.

Step 4: The work role and corresponding definition from SFIA were stated.

Step 5: The coding of the work roles, see Table 24 column 5, was used to match to the work roles from SFIA. Latent and manifest data analysis was applied where the category, code and meaning unit of a specific work role was read and re-read alongside the SFIA defined work roles, and compared and matched. The results from this process can be seen in Table 25. Column 5 of this table indicates the work roles from SFIA which matched to the specific NIST NICE CWF work role and specific cybersecurity consideration.

The gaps identified after step 3 were confirmed through the process of steps 4 and 5. Now, each step is explained by applying the data analysis process to one of the work roles. The example is in reference to item #1 *Risk Management (RSK): Authorising Official*, in Table 24. Figure 40 shows the process which was followed as well as how each step was applied to ultimately match the NIST NICE CWF work role to the SFIA work role for verification and validation.



STEP 1: Category
Securely Provision
Work role from NIST NICE CWF
Risk Management RSK: Authorising Official

STEP 2A: NIST NICE CWF meaning unit
Senior official or executive with the authority to formally assume responsibility for operating an information system at a level of risk that is acceptable

STEP 2B: NIST NICE CWF code
Keyword: risk, management

STEP 5: Match to work roles from SFIA
Use keyword to search possible matches to the work roles from SFIA
Matched:
20 Business risk management
#28 Portfolio management

STEP 5: # 20 Business risk management meaning unit
The development and implementation of company-wide processes and procedures for managing risks to the company's success or integrity, particularly those emerging from the use of information technology, energy supply reductions or outages, or improper disposal of materials, hardware, or data.

STEP 5: #28 Portfolio management meaning unit
The creation and implementation of a systematic management framework for defining and delivering a portfolio of programs, initiatives and/or ongoing services in support of certain corporate strategy and goals. The implementation a strategic investment appraisal and decision-making process based on a clear understanding of cost, risk, interdependencies and influence on existing company activities, allowing measurement and objective evaluation of potential changes and the benefits to be realised. The prioritisation of resource utilisation and the improvements that must be made. Regular review of portfolios. Service pipeline management (planned or in development), service capping.

Interpretation
#20 Managing of risk is used as input to risk responsibility which is done by senior official
#28 Responsible for strategic management framework related to risks which is the responsibility of senior official

Figure 40: Example of how the data analysis process, steps 4 and 5, was followed based on item #1 from Table 24

Figure 40 depicts steps 4 and 5 of how the work role, *Risk Management: Authorising Official,* was verified and validated using SFIA defined work roles. Results from steps 1 and 2 were used to perform steps 4 and 5.

Step 4: SFIA work roles and their corresponding definitions were listed.

Step 5a: The code from step 2b was used to search through the work roles as defined by SFIA. The code matched with two SFIA work roles, namely *#20 Business risk management* and *#28 Portfolio management.*

Step 5b: Latent and manifest analysis was performed by stating the definition of the work role *Risk Management: Authorising Official* as well as the definition of the work roles from SFIA, namely *#20 Business risk management* and *#28 Portfolio management*. The three definitions were compared to each other and interpreted. The interpretation revealed that:

- #20 Managing of risk is an output of the authorising official as it forms part of risk responsibility.
- #28 The responsibility of the strategic management framework related to risks will lie with the *Risk Management: Authorising Official.*

The results of steps 4 and 5 led to the conclusion that the work role *Risk Management: Authorising Official* corresponds to work roles from SFIA, namely *#20 Business risk* *management* and *#28 Portfolio management* and are considered to be verified and validated, shown in green in the table below.

This process was repeated for the 37 work roles identified in Table 24. This process was also applied to the 6 work roles highlighted in orange from Table 24 which were identified as possible gaps. From the verification process, all 6 items matched to a work role from SFIA (see column 5 of Table 25) and were deemed necessary to add to the water sector cybersecurity practitioner framework of South Africa.

Table 25: Verification and validation of NIST NICE CWF defined work roles

1: No.	2: Category	3: Work roles from NIST NICE CWF	4: Cybersecurity considerations for the South African water sector	5: Verification & validation from SFIA
1	Securely Provision	Risk Management (RSK): Authorising Official	2: Risk assessment & management	# 20 Business risk Management #28 Portfolio management
2	Securely Provision	Risk Management (RSK): Security Control Assessor	Risk assessment & management	#61 Service level management
3	Securely Provision	Software Development: Software Developer	Cryptography, design and implementation of improved security systems	#42 Software design #43 Programming/software developer
4	Securely Provision	Software Development: Secure Software Assessor	Cryptography, design and implementation of improved security systems	#46 Data modelling and design
5	Securely Provision	Systems Architecture: Security Architect	Cryptography, design and implementation of improved security systems	#5 Information security
6	Securely Provision	Technology R&D: Research and Development Specialist	Participate in partnership and outreach for information sharing and collaboration	#15 Innovation #16 Research #22 Emerging technology monitoring
7	Securely Provision	Systems Development: Systems Developer	Cryptography, design and implementation of improved security systems	#40 Systems development management #41 Systems design
8	Securely Provision	Test & Evaluation: System Test & Evaluation Specialist		#38 Business process testing #49 Testing #79 Penetration testing
9	Securely Provision	Systems Development: Information Systems Security Developer	Cryptography, design and implementation of improved security systems	#27 Methods and tools
10	Operate and Maintain	Data Administration: Database Administrator	Asset management	#74 Database administration
11	Operate and Maintain	Data Administration: Data Analyst	Asset management	#7 Analytics
12	Operate and Maintain	Knowledge Management: Knowledge Manager	Asset management	#18 Knowledge management
13	Operate and Maintain	Systems Analysis: Systems Security Analyst	Access control	#56 Systems integration and build #64 Asset management #69 Security administration

1: No.	2: Category	3: Work roles from NIST NICE CWF	4: Cybersecurity considerations for the South African water sector	5: Verification & validation from SFIA
14	Oversee and Govern	Legal Advice and Advocacy: Cyber Legal Advisor	Compliance	#9 Information content publishing
15	Oversee and Govern	Legal Advice and Advocacy: Privacy Officer/Privacy Compliance Manager	Compliance	#9 Information content publishing
16	Oversee and Govern	Training, Education and Awareness: Cyber Instructional Curriculum Developer	Human resource security & cybersecurity awareness	#81 Learning and development management #82 Competency assessments
17	Oversee and Govern	Training, Education and Awareness: Cyber Instructor	Human resource security & cybersecurity awareness	#83 Learning design and development #84 Learning delivery #85 Teaching and subject formation
18	Oversee and Govern	Cyber Security Management: Information Systems Security Manager	Governance	#13 IT management
19	Oversee and Govern	Cyber Security Management: Communications Security Manager	Communication security	#48 Network design
20	Oversee and Govern	Strategic Planning and Policy: Cyber Workforce Developer and Manager	Human resource security & cybersecurity awareness	#87 Resourcing #88 Professional development
21	Oversee and Govern	Strategic Planning and Policy: Cyber Policy and Strategy Planner	Governance	#2 Strategic planning
22	Oversee and Govern	Executive Cyber Leadership: Executive Cyber Leadership	Governance	#1 Enterprise IT governance #3 Information governance
23	Oversee and Govern	Program/Project Management and Acquisition: IT Program Auditor	Governance	#4 Information assurance
24	Protect and Defend	Cyber Defence Analysis: Cyber Defence Analyst	Operations security	#44 Real-time/embedded systems development
25	Protect and Defend	Cyber Defence Infrastructure Support: Cyber Defence Infrastructure Support Specialist	Participate in partnership and outreach for information sharing and collaboration	#11 Specialist advice
26	Protect and Defend	Incident Response: Cyber Defence Incident Responder	Business continuity, incidents, emergencies and disaster recovery planning	#79 Incident management
27	Protect and Defend	Vulnerability Assessment and Management: Vulnerability Assessment Analyst	Systems acquisition, development and maintenance	#78 Problem management
28	Analyse	Warning/Threat Analysis: Threat/Warning Analyst	Systems acquisition, development and maintenance	#93 Safety assessments
29	Analyse	Exploitation Analysis: Exploitation Analyst	Systems acquisition, development and maintenance	#8 Data visualisation

1: No.	2: Category	3: Work roles from NIST NICE CWF	4: Cybersecurity considerations for the South African water sector	5: Verification & validation from SFIA
30	Analyse	All-Source Analysis: All-Source Analyst	Systems acquisition, development and maintenance	#26 Data management
31	Analyse	All-Source Analysis: Mission Assessment Specialist	Systems acquisition, development and maintenance	#35 Organisational capability development
32	Analyse	Targets: Target Developer	Systems acquisition, development and maintenance	#34 Requirements definition and management
33	Analyse	Targets: Target Network Analyst	Systems acquisition, development and maintenance	#24 Network planning
34	Analyse	Language Analysis: Multi-Disciplined Language Analyst	Systems acquisition, development and maintenance	#63 Configuration management
35	Collect and Operate	Cyber Operational Planning: Cyber Intel Planner	Business continuity, incidents, emergencies and disaster recovery planning	#27 Methods and tools
36	Collect and Operate	Cyber Operational Planning: Cyber Ops Planner	Business continuity, incidents, emergencies and disaster recovery planning	#3 Information governance #23 Continuity management #27 Methods and tools
37	Collect and Operate	Cyber Operational Planning: Partner Integration Planner	Participate in partnership and outreach for information sharing and collaboration	#10 Consultancy
38	Collect and Operate	Cyber Operations: Cyber Operator	Operations security	#73 IT infrastructure
39	Investigate	Cyber Investigation: Cyber Crime Investigator		#94 Digital forensics
40	Investigate	Digital Forensics: Law Enforcement/Counterintelligence Forensics Analyst		#94 Digital forensics
41	Investigate	Digital Forensics: Cyber Defence Forensics Analyst		#94 Digital forensics
42			Physical & environmental security	#80 Facilities management
43			Securing the supply chain	#96 Supplier management

By following the steps above, a list of 43 work roles were identified for the water sector of South Africa based on the cybersecurity considerations listed in Table 23. However, several gaps have also been identified and are highlighted in orange in Tables 24 and 25.

Gaps identified

Two types of gaps were identified. The first set of gaps related to the water sector cybersecurity considerations. No considerations match the following work roles:

1. *Test & Evaluation: System Test & Evaluation Specialist*
2. *Cyber Investigation: Cyber Crime Investigator*
3. *Digital Forensics: Law Enforcement/Counterintelligence Forensics Analyst*
4. *Digital Forensics: Cyber Defence Forensics Analyst*

The second set of gaps related to the NICE NIST CWF work role. The work roles did not match the following cybersecurity considerations:

1. *Physical & Environmental Security*
2. *Securing the Supply Chain*

The gaps related to the cybersecurity considerations reveal that little emphasis is currently placed on identifying where the cyberthreats emanate from, as well as apprehension of the perpetrators. This is a very important aspect to consider as this will influence consequences applied to cyberattackers and future cybercriminal activity. Gaps related to the defined work roles indicate that third-party cyberattacks are currently not considered as a high risk. Cyberattacks can come from any source and may have a devastating impact on an organisation.

Another gap identified related to the physical security of cybersecurity assets. Hardware can easily be infiltrated by a cyberattacker. To close the gaps related to the cybersecurity consideration, the definitions of the required consideration were adapted from the definition of the work role identified as well as the definition of SFIA. To close the gap related to the defined work roles from NIST NICE CWF, the methodology of creating new work roles was applied by defining the task through adapting a definition from SFIA and the cybersecurity considerations.

6.5 Framework for the work roles of cybersecurity practitioners in South Africa

Building the framework

The previous sections detailed the defining of the water sector cybersecurity considerations and their corresponding work roles. The defined work roles per consideration will now be applied to the water sector organisational structure which was defined by literature. The process flow followed can be seen in Figure 41.

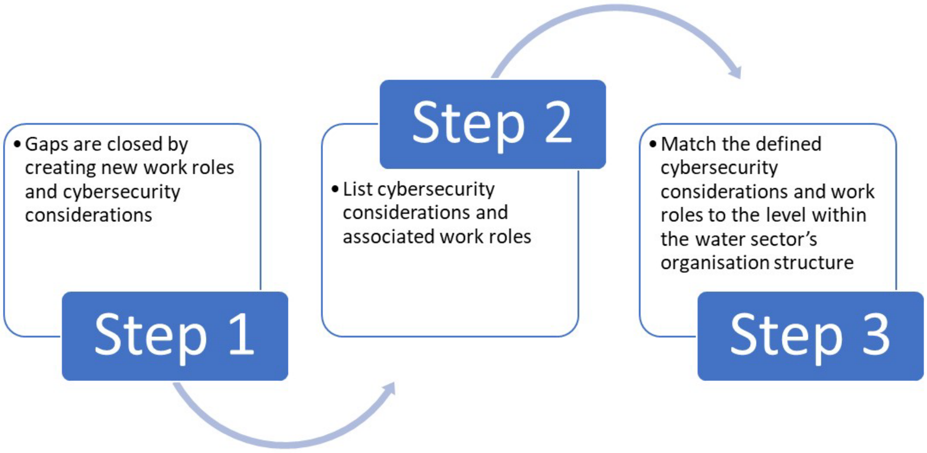

Step 1
• Gaps are closed by creating new work roles and cybersecurity considerations
Step 2
• List cybersecurity considerations and associated work roles
Step 3
• Match the defined cybersecurity considerations and work roles to the level within the water sector's organisation structure

Figure 41: Development of framework process flow diagram

Step 1: As indicated in the previous section, six gaps were identified that needed to be addressed. The NIST NICE CWF describes how to create new work roles by defining the tasks which will describe the work. The cybersecurity considerations can also be assigned based on the description of the consideration.

Step 2: The water sector considerations and associated work roles are listed in Table 24, columns 3 and 6.

Step 3: Each work role was then matched to the level within the hierarchy within the water sector organisational structure based on the roles and responsibilities defined in Figure 36. This was done by conducting latent and manifest analysis of the roles and responsibilities at each hierarchy of the organisational structure and the work role definition. This was then compared and matched.

Closing the gaps

The gaps are split into two types. Type 1 gaps are in terms of the water sector cybersecurity considerations and type 2 gaps are the defined work roles from the NIST NICE CWF. Four gaps were identified as type 1, which can be seen in Table 26 below, extracted from Table 24. The cybersecurity consideration was defined based on the definition of the work role from NIST NICE CWF and the verification definition from SFIA. The cybersecurity considerations, highlighted in orange, which have been assigned for the gaps can be seen in Table 26, column 2.

Table 26: Gaps identified in the water sector's cybersecurity considerations

No. #	Water sector cybersecurity considerations	Work role
8	Cybersecurity testing & evaluation	Test & Evaluation: System Test & Evaluation Specialist
39	Investigation of cybercrimes	Cyber Investigation: Cyber Crime Investigator
40	Forensic analysis and law enforcement liaison for cybercrimes	Digital Forensics: Law Enforcement/Counterintelligence Forensics Analyst
41	Forensic analysis and law enforcement liaison for cybercrimes	Digital Forensics: Cyber Defence Forensics Analyst

Two gaps were identified as type 2, which can be seen in Table 27 below. These gaps were closed by applying the methodology of creating a new work role based on the NIST NICE CWF, which indicates that a new work role can be created by defining the task which will describe the work. Tasks to be performed were adapted from the defined cybersecurity considerations in Table 23 and SFIA work roles.

The tasks associated with the two gaps identified are described as follows:

For item 42, the cybersecurity consideration and SFIA verification #80 were used to describe the task. Item 42 is described as the planning, control and management of all the facilities related to cybersecurity hardware and infrastructure. This includes physical environment provision and management, such as environmental monitoring. Physical access control and adherence to all mandatory health and safety policies and regulations at work are included. Physical access control will be controlled and managed to limit and restrict access only to authorised personnel who need to interface with the hardware, as hackers can swiftly gain access to sensitive data and systems via physical equipment. Physical access will be restricted to IT and ICS settings, as well as communications equipment and assets in remote locations. This work role will be the enforcer.

For item 43, the task was defined as per the cybersecurity consideration and SFIA verification #96. Item 43 is described as the process of balancing costs, efficiency and service quality by aligning an organisation's supplier performance objectives and activities with sourcing strategy and plans. Working relationships built on collaboration, trust and open communication are established with suppliers to enable co-innovation and service improvement. The development of governance documentation, policies and procedures for all supply chain relationships will be required. CSA related to the supply chain needs to be enforced. Regular risk assessments, threats detections and vulnerability assessments on the supply chain relationships must be conducted. Using a set of agreed-upon indicators, performance and risks across multiple vendors (internal and external) must be managed.

The work role is derived from the descriptions above and can be seen in Table 27 below highlighted in orange.

Table 27: Gaps identified in the water sector's cybersecurity considerations

No. #	Water sector cybersecurity considerations	Work role
42	Physical & environmental security	Physical Cyber Security Asset Security Officer
43	Securing the supply chain	Third Party Cyber Security Officer

Framework

The framework was developed by using the results from the content analysis process. The framework incorporates the hierarchy of the water sector organisational structure to indicate which work role needs to be fulfilled by what level within the structure. This is an important step as it indicates how the framework can be applied to the South African water sector's organisational structure.

The organisational hierarchical structure for the water sector of South Africa (see Figure 36) was used to build the framework. Based on the responsibility at each level within the water sector organisational structure, the cybersecurity practitioner work roles and corresponding cybersecurity considerations, the cybersecurity practitioner work roles framework for the water sector of South Africa was developed and can be seen in Table 28.

In Table 28, columns 1 and 2 have been extracted from Table 24. The gaps identified were addressed above and have been included in the framework. Column 3 from Table 26 has been incorporated by performing latent and manifest analysis on the roles and responsibility defined in Figure 36 and matched to a specific work role.

Table 28: Framework for cybersecurity work roles for the water sector of South Africa

Water sector cybersecurity considerations	Work role	Organisational structure level
Governance	Executive Cyber Leadership: Executive Cyber Leadership	Ministerial level
Governance	Strategic Planning and Policy: Cyber Policy and Strategy Planner	Departmental
Human resource security & cybersecurity awareness	Strategic Planning and Policy: Cyber Workforce Developer and Manager	Departmental
Compliance	Legal Advice and Advocacy: Cyber Legal Advisor	National & regional
Compliance	Legal Advice and Advocacy: Privacy Officer/Privacy Compliance Manager	National & regional
Risk assessment & management	Risk Management (RSK): Authorising Official	National & regional
Governance	Conducts evaluations of an IT program or its individual components to determine compliance with published standards	Local
Business continuity, incidents, emergencies and disaster recovery planning	Cyber Operational Planning: Cyber Intel Planner	Local
Business continuity, incidents, emergencies and disaster recovery planning	Cyber Operational Planning: Cyber Ops Planner	Local
Cryptography, design and implementation of improved security systems	Systems Development: Systems Developer	Local
Cryptography, design and implementation of improved security systems	Systems Architecture: Security Architect	Local
Participate in partnership and outreach for information sharing and collaboration	Cyber Operational Planning: Partner Integration Planner	Local
Human resource security & cybersecurity awareness	Training, Education and Awareness: Cyber Instructional Curriculum Developer	Local
Human resource security & cybersecurity awareness	Training, Education and Awareness: Cyber Instructor	Local
Participate in partnership and outreach for information sharing and collaboration	Cyber Defence Infrastructure Support: Cyber Defence Infrastructure Support Specialist	Local
Forensic analysis and law enforcement liaison for cybercrimes	Digital Forensics: Law Enforcement/Counterintelligence Forensics Analyst	Local
Forensic analysis and law enforcement liaison for cybercrimes	Digital Forensics: Cyber Defence Forensics Analyst	Local
Governance	Cyber Security Management: Information Systems Security Manager	Water & wastewater works
Business continuity, incidents, emergencies and disaster recovery planning	Incident Response: Cyber Defence Incident Responder	Water & wastewater works
Risk assessment & management	Risk Management (RSK): Security Control Assessor	Water & wastewater works
Cryptography, design and implementation of improved security systems	Software Development: Software Developer	Water & wastewater works
Cryptography, design and implementation of improved security systems	Software Development: Secure Software Assessor	Water & wastewater works
Participate in partnership and outreach for information sharing and collaboration	Technology R&D: Research and Development Specialist	Water & wastewater works
Cybersecurity testing & evaluation	Test & Evaluation: System Test & Evaluation Specialist	Water & wastewater works
Cryptography, design and implementation of improved security systems	Systems Development: Information Systems Security Developer	Water & wastewater works
Asset management	Data Administration: Database Administrator	Water & wastewater works
Asset management	Data Administration: Data Analyst	Water & wastewater works
Asset management	Knowledge Management: Knowledge Manager	Water & wastewater works
Access control	Systems Analysis: Systems Security Analyst	Water & wastewater works

Water sector cybersecurity considerations	Work role	Organisational structure level
Communication security	Cyber Security Management: Communications Security Manager	Water & wastewater works
Operations security	Cyber Defence Analysis: Cyber Defence Analyst	Water & wastewater works
Systems acquisition, development and maintenance	Vulnerability Assessment and Management: Vulnerability Assessment Analyst	Water & wastewater works
Systems acquisition, development and maintenance	Warning/Threat Analysis: Threat/Warning Analyst	Water & wastewater works
Systems acquisition, development and maintenance	Exploitation Analysis: Exploitation Analyst	Water & wastewater works
Systems acquisition, development and maintenance	All-Source Analysis: All-Source Analyst	Water & wastewater works
Systems acquisition, development and maintenance	All-Source Analysis: Mission Assessment Specialist	Water & wastewater works
Systems acquisition, development and maintenance	Targets: Target Developer	Water & wastewater works
Systems acquisition, development and maintenance	Targets: Target Network Analyst	Water & wastewater works
Systems acquisition, development and maintenance	Language Analysis: Multi-Disciplined Language Analyst	Water & wastewater works
Operations security	Cyber Operations: Cyber Operator	Water & wastewater works
Investigation of cybercrimes	Cyber Investigation: Cyber Crime Investigator	Water & wastewater works
Physical & environmental security	Security Officer	Water & wastewater works
Securing the supply chain	Third Party Cyber Security Officer	Water & wastewater works

As seen in Table 28, all work roles have been defined to a level within the water sector's organisational structure. It should be noted that the framework indicates the minimum work roles required based on the water sector organisational structure developed from literature. The gaps identified in Table 24 have been addressed. The work roles assigned to ministerial, departmental, local and regional are for oversight and governance purposes. The work roles assigned to cybersecurity practitioners within the water and wastewater works are implementational, i.e. all procedures, policies and governances enforced by individuals higher in the hierarchy are performed by practitioners at the water and wastewater works level.

6.6 Recommendations

The work roles defined for cybersecurity practitioners should be filled by the organisation to ensure that prevention, mitigation and detection of cyberthreats occur to reduce this emerging risk. The water sector needs to start sharing experiences of cyberthreats and events across sectors as this will assist in implementing lessons learnt and possibly preventing future incidents. Application of the framework needs to start at ministerial level where legislation must be developed, reviewed and implemented and a clear plan for implementation also developed. Departmental level of the water sector ensures that the legislation, policies and procedures are governed and enforced by measuring compliance. This level must also ensure that resources are made available to carry out the required cybersecurity practitioner work roles. National and regional levels of the water sector must ensure the development of procedures and their management. Local level must ensure that policies and procedures are carried out correctly within their jurisdiction. Plant level must ensure that legislation, policies and procedures are carried out.

An assessment of the educational programmes needed to be done to ensure alignment with the required work roles for the sector. This assessment is reported on in the next chapter.

7 SPECIALISED SKILLS AND KNOWLEDGE REQUIRED

Considering the water sector cybersecurity considerations identified in the previous chapter, an assessment of the educational programmes was done to ensure alignment with work roles for the sector. The provision of training to existing staff members who will fill the identified work roles in the water sector is an important step towards ensuring the cybersecurity of the sector.

The following important aspects were considered:

- All certificates considered had to be internationally recognised.
- Vendors were considered who offer virtual/online training globally, which includes:
  - Certification exams – Online or at local test centre
  - Prep courses: Online and classroom available

The water sector cybersecurity considerations and work roles which were identified in the previous chapter, included in Table 29, were used as a guide to find appropriate professional certifications related to the considerations.

Table 29: Professional certification table linked to cybersecurity work roles

Water sector cybersecurity considerations	Work roles	Certification	Description	Professional body accrediting certification	Local training vendors	Link
Access control	Systems Analysis: Systems Security Analyst	Certified Data Privacy Solutions Engineer (CDPSE)	Data scientists/analysts that mine and analyse data for customer insights, as well as IT professionals that create and implement technical privacy solutions.	ISACA	**Firebrand** https://firebrand.training/en	https://www.isaca.org/credentialing/certified-data-privacy-solutions-engineer
		Certified Information System Auditor (CISA)	To understand and ensure that an organisation's security policies, standards, procedures and controls are aligned and effectively protect the confidentiality, integrity and availability of the organisation's information assets.	ISACA	**Firebrand** https://firebrand.training/en **Koenig SA** – https://koenig-solutionsdl.azurewebsites.net/isaca-information-systems-audit-control-association-training-courses **Enterprise Governance of IT (EGIT)** – https://www.egit.co.za/	https://www.isaca.org/credentialing/cisa
		CMIITPSA – Certified Member of IITPSA	The IITPSA's Certified Member distinction ensures that practitioners accepted to this professional designation have the necessary qualifications and demonstrate a sufficient level of relevant professional experience in one or more of the various disciplines that fall under the ICT umbrella. Software, network, or telecommunications engineering, information security, ICT governance, business analysis, database management and administration, ICT lecturing and/or research, project management, business intelligence, software design and/or development, software testing/quality assurance, web development and mobile technologies are just a few examples of such disciplines.	IITPSA	Deviare – https://deviare.africa/ Joburg Centre of Software Engineering (JCSE) – https://jcse.org.za/ Mobile Applications Laboratory NPC (Mlab) – https://mlab.co.za/programmes/ Regenesys Business School – https://regenesys.net/	https://www.iitpsa.org.za/certified-member-cmiitpsa/
Asset management	1. Data Administration: Database Administrator 2. Data Administration: Data Analyst 3. Knowledge Management: Knowledge Manager 4. ICS security: Cybersecurity Practices for Industrial Control Systems	Certified Data Privacy Solutions Engineer (CDPSE)	IT professionals engaged in creating and implementing technical privacy solutions and data scientists/analysts that mine and analyse data for customer insights.	ISACA	**Firebrand** https://firebrand.training/en	https://www.isaca.org/credentialing/certified-data-privacy-solutions-engineer
		CMIITPSA – Certified Member of IITPSA	Certified Member designation of the IITPSA ensures that practitioners admitted to this professional designation have appropriate qualifications and demonstrate a sufficient degree of relevant professional experience in one or more of the many disciplines included within the ICT spectrum. Such disciplines include (but are not limited to) software, network or telecommunications engineering, information security, ICT governance, business analysis, database management and administration, ICT lecturing and/or research, project management, business intelligence, software design and/or development, software testing/quality assurance, web development and mobile technologies.	IITPSA	Deviare – https://deviare.africa/ Joburg Centre of Software Engineering (JCSE) – https://jcse.org.za/ Mobile Applications Laboratory NPC (Mlab) – https://mlab.co.za/programmes/ Regenesys Business School – https://regenesys.net/	https://www.iitpsa.org.za/certified-member-cmiitpsa/

Water sector cybersecurity considerations	**Work roles**	**Certification**	**Description**	**Professional body accrediting certification**	**Local training vendors**	**Link**
		IT Asset Management Certification （IAITAM）	IAITAM is a demonstration of specialist knowledge of IT asset management. Support significant cost savings and better management of IT assets. Ensure proper disposal of retired IT assets in a time of increased regulatory requirements. Establish the optimum level of maintenance agreements, software licence agreements and negotiate better pricing and terms.	APMG International	**RADtech —** https://rad-tech.co.za/__trashed-3/ **QA （International online only） —** https://www.qa.com/course-catalogue/courses/certificate-in-digital-forensics-fundamentals-qaidigfor?learningMethod=Virtual&	https://apmg-international.com/product/iaitam-certifications
		Certified Asset Management Professional （CAMP）	This covers the 12 key process areas （KPAs） in the IAITAM Best Practice Library, the roles and responsibilities that affect an ITAM programme, core functional areas, KPA indicators, strategic positioning, and how ITAM can be integrated into other frameworks like ITSM so that they work together in the most efficient way for an organisation, resulting in a higher return on investment （ROI） for its IT portfolio.	APMG International	**RADtech —** https://rad-tech.co.za/__trashed-3/ **QA （International online only） —** https://www.qa.com/course-catalogue/courses/certificate-in-digital-forensics-fundamentals-qaidigfor?learningMethod=Virtual&	https://apmg-international.com/product/iaitam-certifications
		Certified Hardware Asset Management Professional （CHAMP）	Designing the architecture for an IT hardware asset management programme is possible with CHAMP accreditation. The assessment and application of an organisation's function area needs in support of the IT hardware asset management programme. Organisational requirements for the IT hardware asset management programme are developed. Technology auditing procedures are integrated with parts of hardware asset management. Processes for managing IT hardware assets are evaluated. Different techniques to improve an IT hardware asset management programme are developed. The development of a plan and policies for an IT hardware asset management programme.	APMG International	**RADtech —** https://rad-tech.co.za/__trashed-3/ **QA （International online only） —** https://www.qa.com/course-catalogue/courses/certificate-in-digital-forensics-fundamentals-qaidigfor?learningMethod=Virtual&	https://apmg-international.com/product/iaitam-certifications
		Certified Software Asset Manager （CSAM）	For new IT asset managers and other IT professionals working in asset management, resource budgeting, finance, software licensing, contract management and strategic planning, CSAM is a must-have course.	APMG International	**RADtech —** https://rad-tech.co.za/__trashed-3/ **QA （International online only） —** https://www.qa.com/course-catalogue/courses/certificate-in-digital-forensics-fundamentals-qaidigfor?learningMethod=Virtual&	https://apmg-international.com/product/iaitam-certifications
		Certified IT Asset Disposal （CITAD）	CITAD is required reading for IT asset disposal programme managers and other IT professionals involved in asset management, resource budgeting, finance, software licensing, contract management and strategic planning.	APMG International	**RADtech —** https://rad-tech.co.za/__trashed-3/ **QA （International online only） —** https://www.qa.com/course-catalogue/courses/certificate-in-digital-	https://apmg-international.com/product/iaitam-certifications

Water sector cybersecurity considerations	Work roles	Certification	Description	Professional body accrediting certification	Local training vendors	Link
					forensics-fundamentals-qaidigfor?learningMethod=Virtual&	
		Certified Mobility Asset Management （CMAM）	This is for people in a company who are responsible for maintaining and accounting for mobile devices, as well as ensuring the efficiency benefits and mitigating the risk that mobility poses to the organisation.	APMG International	**RADtech —** https://rad-tech.co.za/__trashed-3/ **QA （International online only） —** https://www.qa.com/course-catalogue/courses/certificate-in-digital-forensics-fundamentals-qaidigfor?learningMethod=Virtual&	https://apmg-international.com/product/iaitam-certifications
		Certified IT Asset Manager （CITAM）	For individuals entrusted with establishing an ITAM programme from the ground up at their organisation or experienced ITAM candidates wishing to improve their ITAM programme in practical and scalable ways.	APMG International	**RADtech —** https://rad-tech.co.za/__trashed-3/ **QA （International online only） —** https://www.qa.com/course-catalogue/courses/certificate-in-digital-forensics-fundamentals-qaidigfor?learningMethod=Virtual&	https://apmg-international.com/product/iaitam-certifications
		Cybersecurity Practices for Industrial Control Systems	Range of offerings on Cybersecurity Practices for Industrial Control Systems	Cybersecurity and Infrastructure Security Agency （CISA）	https://ics-training.inl.gov/pages/6/cisa-dashboard	https://ics-training.inl.gov/pages/6/cisa-dashboard
Business continuity, incidents, emergencies and disaster recovery planning	1. Cyber Operational Planning: Cyber Intel Planner 2. Cyber Operational Planning: Cyber Ops Planner 3. Incident Response: Cyber Defence Incident Responder	Certified Data Privacy Solutions Engineer （CDPSE）	Data scientists/analysts that mine and analyse data for customer insights, as well as IT professionals that create and implement technical privacy solutions.	ISACA	**Firebrand** https://firebrand.training/en	https://www.isaca.org/credentialing/certified-data-privacy-solutions-engineer
		CMIITPSA – Certified Member of IITPSA	The IITPSA's Certified Member distinction ensures that practitioners accepted to this professional designation have the necessary qualifications and demonstrate a sufficient level of relevant professional experience in one or more of the various disciplines that fall under the ICT umbrella. Software, network, or telecommunications engineering, information security, ICT governance, business analysis, database management and administration, ICT lecturing and/or research, project management, business intelligence, software design and/or development, software testing/quality assurance, web development and mobile technologies are just a few examples of such disciplines.	IITPSA	**Deviare** - https://deviare.africa/ **Joburg Centre of Software Engineering （JCSE）** - https://jcse.org.za/ **Mobile Applications Laboratory NPC （Mlab）** - https://mlab.co.za/programmes/ **Regenesys Business School** - https://regenesys.net/	https://www.iitpsa.org.za/certified-member-cmiitpsa/
		Cybersecurity Nexus （CSX）	The CSX and CSX-P examine one's ability to conduct globally verified cybersecurity skills encompassing five security functions developed from	ISACA	**CSX （Online only）** - https://nexus.isaca.org/products	https://www.isaca.org/credentialing/cybersecurity

Water sector cybersecurity considerations	Work roles	Certification	Description	Professional body accrediting certification	Local training vendors	Link
		CSX Cybersecurity Practitioner Certificate （CSX-P）	the NIST Cybersecurity Framework: Identify, protect, detect, respond and recover.	ISACA	**Koenig SA** - https://koenig-solutionsdl.azurewebsites.net/isaca-information-systems-audit-control-association-training-courses	https://www.isaca.org/credentialing/csx-p
Communication security	Cyber Security Management: Communications Security Manager	IT Risk Fundamentals Certificate	The IT Risk Fundamentals Certificate and accompanying training are designed for professionals who want to learn about risk and I&T-related risk, who work with risk professionals, or who are new to risk and want to work in the risk or IT risk profession.	ISACA	**Firebrand** https://firebrand.training/en **Koenig SA** - https://koenig-solutionsdl.azurewebsites.net/isaca-information-systems-audit-control-association-training-courses **Enterprise Governance of IT （EGIT）** - https://www.egit.co.za/	https://www.isaca.org/credentialing/it-risk-fundamentals-certificate
		Certified in Risk and Information Systems Control （CRISC）	CRISC validates experience in building a well-defined, agile risk-management programme, based on best practices to identify, analyse, evaluate, assess, prioritise and respond to risks.	ISACA	**Firebrand** https://firebrand.training/en **Enterprise Governance of IT （EGIT）** - https://www.egit.co.za/	https://www.isaca.org/credentialing/crisc
		CMIITPSA – Certified Member of IITPSA	The IITPSA's Certified Member distinction ensures that practitioners accepted to this professional designation have the necessary qualifications and demonstrate a sufficient level of relevant professional experience in one or more of the various disciplines that fall under the ICT umbrella. Software, network, or telecommunications engineering, information security, ICT governance, business analysis, database management and administration, ICT lecturing and/or research, project management, business intelligence, software design and/or development, software testing/quality assurance, web development and mobile technologies are just a few examples of such disciplines.	IITPSA	**Deviare** - https://deviare.africa/ **Joburg Centre of Software Engineering （JCSE）** - https://jcse.org.za/ **Mobile Applications Laboratory NPC （Mlab）** - https://mlab.co.za/programmes/ **Regenesys Business School** - https://regenesys.net/	https://www.iitpsa.org.za/certified-member-cmiitpsa/
Compliance	1. Legal Advice and Advocacy: Cyber Legal Advisor 2. Legal Advice and Advocacy: Privacy Officer/Privacy Compliance Manager	Certified Information Systems Auditor （CISA）	CISA gives businesses a valid and trustworthy way to find engineers who are capable of embedding privacy by design into technology platforms, products and processes, connecting with legal specialists and keeping the company compliant in a timely and cost-effective manner.	ISACA	**Firebrand** https://firebrand.training/en **Koenig SA** - https://koenig-solutionsdl.azurewebsites.net/isaca-information-systems-audit-control-association-training-courses **Enterprise Governance of IT （EGIT）** - https://www.egit.co.za/	https://www.isaca.org/credentialing/cisa
		Cybersecurity Audit Certificate	ISACA's Cybersecurity Audit Certificate equips audit/assurance professionals with the skills they need to perform well in cybersecurity audits, as well as IT risk managers with a grasp of cyber-related risk and mitigation strategies.	ISACA	**Firebrand** https://firebrand.training/en	https://www.isaca.org/credentialing/cybersecurity-audit-certificate
		CMIITPSA – Certified Member of IITPSA	The IITPSA's Certified Member distinction ensures that practitioners accepted to this professional designation have the necessary qualifications and demonstrate a sufficient level of relevant professional	IITPSA	**Deviare** - https://deviare.africa/	https://www.iitpsa.org.za/certified-member-cmiitpsa/

Water sector cybersecurity considerations	Work roles	Certification	Description	Professional body accrediting certification	Local training vendors	Link
			experience in one or more of the various disciplines that fall under the ICT umbrella. Software, network, or telecommunications engineering, information security, ICT governance, business analysis, database management and administration, ICT lecturing and/or research, project management, business intelligence, software design and/or development, software testing/quality assurance, web development and mobile technologies are just a few examples of such disciplines.		**Joburg Centre of Software Engineering （JCSE）** – https://jcse.org.za/ **Mobile Applications Laboratory NPC （Mlab）** – https://mlab.co.za/programmes/ **Regenesys Business School** – https://regenesys.net/	
Cryptography, design and implementation of improved security systems	1. Systems Development: Systems Developer 2. Systems Architecture: Security Architect 3. Software Development: Software Developer 4. Software Development: Secure Software Assessor 5. Systems Development: Information Systems Security Developer	Certified Data Privacy Solutions Engineer （CDPSE）	Data scientists/analysts that mine and analyse data for customer insights, as well as IT professionals that create and implement technical privacy solutions.	ISACA	**Firebrand** https://firebrand.training/en	https://www.isaca.org/credentialing/certified-data-privacy-solutions-engineer
		CMIITPSA – Certified Member of IITPSA	The IITPSA's Certified Member distinction ensures that practitioners accepted to this professional designation have the necessary qualifications and demonstrate a sufficient level of relevant professional experience in one or more of the various disciplines that fall under the ICT umbrella. Software, network, or telecommunications engineering, information security, ICT governance, business analysis, database management and administration, ICT lecturing and/or research, project management, business intelligence, software design and/or development, software testing/quality assurance, web development and mobile technologies are just a few examples of such disciplines.	IITPSA	**Deviare** – https://deviare.africa/ **Joburg Centre of Software Engineering （JCSE）** – https://jcse.org.za/ **Mobile Applications Laboratory NPC （Mlab）** – https://mlab.co.za/programmes/ **Regenesys Business School** – https://regenesys.net/	https://www.iitpsa.org.za/certified-member-cmiitpsa/
		Cybersecurity Nexus （CSX）	The CSX and CSX-P examine one's ability to conduct globally verified cybersecurity skills encompassing five security functions developed from the NIST Cybersecurity Framework: Identify, protect, detect, respond and recover.	ISACA	**CSX （Online only）** – https://nexus.isaca.org/products **Koenig SA** – https://koenig-solutionsdl.azurewebsites.net/isaca-information-systems-audit-control-association-training-courses	https://www.isaca.org/credentialing/cybersecurity
		CSX Cybersecurity Practitioner Certificate （CSX-P）		ISACA		https://www.isaca.org/credentialing/csx-p
		Certified in Emerging Technology Certification （CET）	Provides the skills to apply in-demand emerging tech expertise to current or prospective employment in IT audit, risk, security, cybersecurity, governance, privacy, business development and other areas. CET's four certificates add up to a certification that certifies capacity to do technical tasks and advise on, appraise and apply emerging technologies, providing more than simply a theoretical grasp.	ISACA	**Firebrand** https://firebrand.training/en	https://www.isaca.org/credentialing/cet
Cybersecurity testing & evaluation	Test & Evaluation: System Test & Evaluation Specialist	Cybersecurity Nexus （CSX）	The CSX and CSX-P examine one's ability to conduct globally verified cybersecurity skills encompassing five security functions developed from the NIST Cybersecurity Framework: Identify, protect, detect, respond and recover.	ISACA	**CSX （Online only）** – https://nexus.isaca.org/products **Koenig SA** – https://koenig-solutionsdl.azurewebsites.net/isaca-information-systems-audit-control-association-training-courses	https://www.isaca.org/credentialing/cybersecurity
		CSX Cybersecurity Practitioner Certificate （CSX-P）		ISACA		https://www.isaca.org/credentialing/csx-p

Water sector cybersecurity considerations	Work roles	Certification	Description	Professional body accrediting certification	Local training vendors	Link
Forensic analysis and law enforcement liaison for cybercrimes	1. Digital Forensics: Law Enforcement/ Counterintelligence Forensics Analyst 2. Digital Forensics: Cyber Defence Forensics Analyst	Certified Information Systems Auditor (CISA)	CISA gives businesses a valid and trustworthy way to find engineers who are capable of embedding privacy by design into technology platforms, products and processes, connecting with legal specialists and keeping the company compliant in a timely and cost-effective manner.	ISACA	**Firebrand** https://firebrand.training/en **Koenig SA** - https://koenig-solutionsdl.azurewebsites.net/isaca-information-systems-audit-control-association-training-courses **Enterprise Governance of IT (EGIT)** - https://www.egit.co.za/	https://www.isaca.org/credentialing
		Certified Information Systems Security Professional (CISSP)	Computer forensic examiners should be certified exclusively on the basis of their knowledge and practical examination skills and abilities as they apply to digital forensics.	IISSCC	**Torquelt** - https://www.torque-it.com/contact-us	https://www.isc2.org/Certifications/CISSP
		Certified Computer Examiner (CCE)	Professionals have the knowledge, skills and abilities to conduct formal incident investigations and respond to complex incident scenarios.	ISFCE	**ISFCE Training Provider (Online only)** Computer Forensic Training Center Online - https://www.cftco.com/ SANS - https://forensics.sans.org/	https://www.isfce.com/certification.htm
		Certified Forensic Computer Examiner (CFCE)	CFCE is based on a series of core competencies in the field of computer/digital forensics.	ISFCE	**ISFCE Training Provider (Online only)** **Computer Forensic Training Center Online** - https://www.cftco.com/ **SANS** - https://forensics.sans.org/	https://www.isfce.com/certification.htm
		Global Information Assurance Certification (GIAC)	GIAC is an information security certification entity that specialises in technical and practical certification as well as new research.	ISFCE SANS	***ISFCE Training Provider (Online only)*** **Computer Forensic Training Center Online** - https://www.cftco.com/ **SANS** - https://forensics.sans.org/	https://www.isfce.com/certification.htm https://www.giac.org/get-certified/?msc=main-nav
		GIAC Certified Forensic Analyst (GCFA)	GCFA is a vendor-neutral certification that assesses a candidate's knowledge and skills in computer forensics, information security and incident response.	ISFCE	**ISFCE Training Provider (Online only)** **Computer Forensic Training Center Online** - https://www.cftco.com/ **SANS** - https://forensics.sans.org/	https://www.isfce.com/certification.htm https://www.giac.org/get-certified/?msc=main-nav
		GIAC Advanced Smartphone Forensics (GASF)	GIAC is a company that specialises in technical and practical certification as well as new research in the field of information security.	ISFCE	**ISFCE Training Provider (Online only)** **Computer Forensic Training Center Online** - https://www.cftco.com/ **SANS** - https://forensics.sans.org/	https://www.isfce.com/certification.htm https://www.giac.org/get-certified/?msc=main-nav
		GIAC Certified Forensic Examiner (GCFE)	The GCFE is a credential that verifies a practitioner's understanding of computer forensics.	ISFCE	**ISFCE Training Provider (Online only)** **Computer Forensic Training Center Online** - https://www.cftco.com/ **SANS** - https://forensics.sans.org/	https://www.isfce.com/certification.htm https://www.giac.org/get-certified/?msc=main-nav

Water sector cybersecurity considerations	Work roles	Certification	Description	Professional body accrediting certification	Local training vendors	Link
		GIAC Network Forensic Analyst （GNFA）	The GNFA certification confirms a practitioner's ability to conduct network forensic artefact analysis examinations. The principles of network forensics, normal and abnormal situations for common network protocols, techniques and tools used to evaluate device and system logs, and wireless communication and encrypted protocols have all been shown by GNFA certification holders.	ISFCE	***ISFCE Training Provider （Online only）*** **Computer Forensic Training Center Online –** https://www.cftco.com/ **SANS** – https://forensics.sans.org/	https://www.isfce.com/certification.htm https://www.giac.org/get-certified/?msc=main-nav
		GIAC Reverse Engineering Malware （GREM）	The GREM certification is for technologists who defend organisations against malicious code. Malicious software （malware） that targets common platforms, such as Microsoft Windows and web browsers, can be reverse-engineered by GREM-certified technologists. In the context of forensic investigations, incident response and Windows system administration, these professionals know how to study the inner workings of malware. By highlighting cutting-edge malware research skills with the GREM certification, technologists can make themselves more useful to their employer and/or customers.	ISFCE	***ISFCE Training Provider （Online Ooly）*** **Computer Forensic Training Center Online –** https://www.cftco.com/ **SANS –** https://forensics.sans.org/	https://www.isfce.com/certification.htm https://www.giac.org/get-certified/?msc=main-nav
		GIAC Security Essentials （GSEC）	The GSEC certification verifies a practitioner's understanding of information security concepts and terminology beyond the basics. Holders of the GSEC certification show that they can perform security activities in hands-on IT systems.	ISFCE	**ISFCE Training Provider （Online only）** **Computer Forensic Training Center Online –** https://www.cftco.com/ **SANS –** https://forensics.sans.org/	https://www.isfce.com/certification.htm https://www.giac.org/get-certified/?msc=main-nav
		CMIITPSA – Certified Member of IITPSA	The IITPSA's Certified Member distinction ensures that practitioners accepted to this professional designation have the necessary qualifications and demonstrate a sufficient level of relevant professional experience in one or more of the various disciplines that fall under the ICT umbrella. Software, network, or telecommunications engineering, information security, ICT governance, business analysis, database management and administration, ICT lecturing and/or research, project management, business intelligence, software design and/or development, software testing/quality assurance, web development and mobile technologies are just a few examples of such disciplines.	IITPSA	**Deviare** – https://deviare.africa/ **Joburg Centre of Software Engineering （JCSE） –** https://jcse.org.za/ **Mobile Applications Laboratory NPC （Mlab） –** https://mlab.co.za/programmes/ **Regenesys Business School –** https://regenesys.net/	https://www.iitpsa.org.za/certified-member-cmiitpsa/

Water sector cybersecurity considerations	Work roles	Certification	Description	Professional body accrediting certification	Local training vendors	Link
		Certification in Digital Forensics Fundamentals （QAIDIGFOR）	The QAIDIGFOR training is meant to assist commercial and government organisations in collecting, preserving and reporting on digital artefacts in a form that is appropriate for use in investigations.	APMG International	**RADtech** – https://rad-tech.co.za/__trashed-3/ **QA （International online only）** – https://www.qa.com/course-catalogue/courses/certificate-in-digital-forensics-fundamentals-qaidigfor?learningMethod=Virtual&	https://apmg-international.com/product/ncsc-certified-training/certificate-digital-forensics-fundamentals
Governance	1. Executive Cyber Leadership: Executive Cyber Leadership 2. Strategic Planning and Policy: Cyber Policy and Strategy Planner 3. Cyber security Management: Information Systems Security Manager 4. Cyber Security Management: Information Systems Security Manager	Certified in Governance of Enterprise IT （CGEIT）	The only individual IT governance certification that is framework independent.	ISACA	**Firebrand** https://firebrand.training/en	https://www.isaca.org/credentialing/cgeit?utm_source=google&utm_medium=cpc&utm_campaign=CertBAU&utm_content=sem_CertBAU_certification-cgeit-africa-exam-google&cid=sem_2006795&Appeal=sem&gclid=Cj0KCQiAgP6PBhDmARIsAPWMq6lhIaGA_jbHU-F_FC798iFQ2zbdqMnu0q-vqpvwLDW1apLdR-DO6aEaAmPKEALw_wcB
		Control Objectives for Information and Related Technologies （COBIT）	COBIT 5 certifications place holders among the best-qualified enterprise IT governance specialists in the world.	ISACA	**Firebrand** https://firebrand.training/en **TorqueIt** – https://www.torque-it.com/contact-us **Koenig SA** – https://koenig-solutionsdl.azurewebsites.net/isaca-information-systems-audit-control-association-training-courses **Enterprise Governance of IT （EGIT）** – https://www.egit.co.za/	https://www.isaca.org/credentialing/cobit/cobit-5-certifcates
		Certified Information Security Manager （CISM）	Expertise in information security governance, program development and management, incident management and risk management is demonstrated by certification.	ISACA	**Firebrand** https://firebrand.training/en **Simpl!learn** – https://www.simplilearn.com/cyber-security **Koenig SA** – https://koenig-solutionsdl.azurewebsites.net/isaca-information-systems-audit-control-association-training-courses	https://www.isaca.org/credentialing/cism

Water sector cybersecurity considerations	Work roles	Certification	Description	Professional body accrediting certification	Local training vendors	Link
		The Chartered Chief Information Officer, South Africa: C-CIO （SA）	The professional designation for chief information officers certified on the NQF is Certified Information Technology Business Professional CITBP （SA）. The CIO is the executive in charge of an organisation's IT strategy and the computer systems needed to support the organisation's particular objectives and goals.	ICITP	**WITS** – https://www.wits.ac.za/linkcentre/cio/	https://www.icitp.org.za/the-chartered-chief-information-officer-south-africa-c-cio-sa/
		CMIITPSA – Certified Member of IITPSA	The IITPSA's Certified Member distinction ensures that practitioners accepted to this professional designation have the necessary qualifications and demonstrate a sufficient level of relevant professional experience in one or more of the various disciplines that fall under the ICT umbrella. Software, network, or telecommunications engineering, information security, ICT governance, business analysis, database management and administration, ICT lecturing and/or research, project management, business intelligence, software design and/or development, software testing/quality assurance, web development and mobile technologies are just a few examples of such disciplines.	IITPSA	**Deviare** – https://deviare.africa/ **Joburg Centre of Software Engineering （JCSE）** – https://jcse.org.za/ **Mobile Applications Laboratory NPC （Mlab）** – https://mlab.co.za/programmes/ **Regenesys Business School** – https://regenesys.net/	https://www.iitpsa.org.za/certified-member-cmiitpsa/
Human resource security & cybersecurity awareness	1. Strategic Planning and Policy: Cyber Workforce Developer and Manager 2. Training, Education and Awareness: Cyber Instructional Curriculum Developer 3. Training, Education and Awareness: Cyber Instructor	CMIITPSA – Certified Member of IITPSA	The IITPSA's Certified Member certification ensures that practitioners admitted to this professional distinction have the necessary qualifications and expertise in one or more of the various disciplines that make up the ICT spectrum. Software, network, or telecommunications engineering, information security, ICT governance, business analysis, database management and administration, ICT lecturing and/or research, project management, business intelligence, software design and/or development, software testing/quality assurance, web development and mobile technologies are just a few examples of such disciplines.	IITPSA	**Deviare** – https://deviare.africa/ **Joburg Centre of Software Engineering （JCSE）** – https://jcse.org.za/ **Mobile Applications Laboratory NPC （Mlab）** – https://mlab.co.za/programmes/ **Regenesys Business School** – https://regenesys.net/	https://www.iitpsa.org.za/certified-member-cmiitpsa/
Investigation of cybercrimes	Cyber Investigation: Cyber Crime Investigator	CMIITPSA – Certified Member of IITPSA	The IITPSA's Certified Member distinction ensures that practitioners accepted to this professional designation have the necessary qualifications and demonstrate a sufficient level of relevant professional experience in one or more of the various disciplines that fall under the ICT umbrella. Software, network, or telecommunications engineering, information security, ICT governance, business analysis, database management and administration, ICT lecturing and/or research, project management, business intelligence, software design and/or development, software testing/quality assurance, web development and mobile technologies are just a few examples of such disciplines.	IITPSA	**Deviare** – https://deviare.africa/ **Joburg Centre of Software Engineering （JCSE）** – https://jcse.org.za/ **Mobile Applications Laboratory NPC （Mlab）** – https://mlab.co.za/programmes/ **Regenesys Business School** – https://regenesys.net/	https://www.iitpsa.org.za/certified-member-cmiitpsa/
Operations security	1. Cyber Defence Analysis: Cyber Defence Analyst	Certified Data Privacy Solutions Engineer （CDPSE）	Data scientists/analysts that mine and analyse data for customer insights, as well as IT professionals that create and implement technical privacy solutions.	ISACA	**Firebrand** https://firebrand.training/en	https://www.isaca.org/credentialing/certified-data-privacy-solutions-engineer

Water sector cybersecurity considerations	Work roles	Certification	Description	Professional body accrediting certification	Local training vendors	Link
	2. Cyber Operations: Cyber Operator 3. Cybersecurity Analyst					
		CMIITPSA – Certified Member of IITPSA	Certified Member designation of the IITPSA ensures that practitioners admitted to this professional designation have appropriate qualifications and demonstrate a sufficient degree of relevant professional experience in one or more of the many disciplines included within the ICT spectrum. Such disciplines include （but are not limited to） software, network or telecommunications engineering, information security, ICT governance, business analysis, database management and administration, ICT lecturing and/or research, project management, business intelligence, software design and/or development, software testing/quality assurance, web development and mobile technologies.	IITPSA	**Deviare** - https://deviare.africa/ **Joburg Centre of Software Engineering （JCSE） -** https://jcse.org.za/ **Mobile Applications Laboratory NPC （Mlab） -** https://mlab.co.za/programmes/ **Regenesys Business School -** https://regenesys.net/	https://www.iitpsa.org.za/certified-member-cmiitpsa/
		CompTIA CySA+	CompTIA Cybersecurity Analyst （CySA+） is an IT workforce certification that applies behavioural analytics to networks and devices to prevent, detect and combat cybersecurity threats through continuous security monitoring.	CompTIA	**CompTIA:** https://www.comptia.org/certifications/cybersecurity-analyst	https://www.comptia.org/certifications/cybersecurity-analyst
Participate in partnership and outreach for information sharing and collaboration	1. Cyber Operational Planning: Partner Integration Planner 2. Cyber Defence Infrastructure Support: Cyber Defence Infrastructure Support Specialist 3. Technology R&D: Research and Development Specialist	Certified in Emerging Technology Certification （CET）	CET affirms that the learner has what it takes to apply in-demand emerging tech expertise to current or future roles in IT audit, risk, security, cybersecurity, governance, privacy, business development and beyond. Offering more than just an understanding of theory and concepts, CET's four certificates stack up to a certification that validates ability to perform technical tasks and advise on, assess and implement emerging technologies	ISACA	**Firebrand** https://firebrand.training/en	https://www.isaca.org/credentialing/cet
		CMIITPSA – Certified Member of IITPSA	Certified Member designation of the IITPSA ensures that practitioners admitted to this professional designation have appropriate qualifications and demonstrate a sufficient degree of relevant professional experience in one or more of the many disciplines included within the ICT spectrum. Such disciplines include （but are not limited to） software, network or telecommunications engineering, information security, ICT governance, business analysis, database management and administration, ICT lecturing and/or research, project management, business intelligence, software design and/or development, software testing/quality assurance, web development and mobile technologies.	IITPSA	**Deviare** - https://deviare.africa/ **Joburg Centre of Software Engineering （JCSE） -** https://jcse.org.za/ **Mobile Applications Laboratory NPC （Mlab） -** https://mlab.co.za/programmes/ **Regenesys Business School -** https://regenesys.net/	https://www.iitpsa.org.za/certified-member-cmiitpsa/
Physical & environmental security	Security Officer	Certified Information Security Manager （CISM）	Certification indicates expertise in information security governance, program development and management, incident management and risk management.	ISACA	**Firebrand** https://firebrand.training/en **Simpl!learn** - https://www.simplilearn.com/cyber-security **Enterprise Governance of IT （EGIT）** - https://www.egit.co.za/	https://www.isaca.org/credentialing/cism
		CMIITPSA – Certified Member of IITPSA	Certified Member designation of the IITPSA ensures that practitioners admitted to this professional designation have appropriate qualifications and demonstrate a sufficient degree of relevant professional experience	IITPSA	**Deviare** - https://deviare.africa/	https://www.iitpsa.org.za/certified-member-cmiitpsa/

Water sector cybersecurity considerations	Work roles	Certification	Description	Professional body accrediting certification	Local training vendors	Link
			in one or more of the many disciplines included within the ICT spectrum. Such disciplines include (but are not limited to) software, network or telecommunications engineering, information security, ICT governance, business analysis, database management and administration, ICT lecturing and/or research, project management, business intelligence, software design and/or development, software testing/quality assurance, web development and mobile technologies.		**Joburg Centre of Software Engineering (JCSE) –** https://jcse.org.za/ **Mobile Applications Laboratory NPC (Mlab) –** https://mlab.co.za/programmes/ **Regenesys Business School –** https://regenesys.net/	
Risk assessment & management	1. Risk Management (RSK): Authorising Official 2. Risk Management (RSK): Security Control Assessor	Cybersecurity Practitioners Certification (CSX-P)	Certification measures one's ability to conduct globally verified cybersecurity skills across five security functions drawn from the NIST Cybersecurity Framework: Identify, protect, detect, respond and recover.	ISACA	**CSX (Online only) –** https://nexus.isaca.org/products **Koenig SA** – https://koenig-solutionsdl.azurewebsites.net/isaca-information-systems-audit-control-association-training-courses	https://www.isaca.org/credentialing/csx-p
		Certified Information Security Manager (CISM)	Expertise in information security governance, program development and management, incident management and risk management is demonstrated by certification.	ISACA	**Firebrand** https://firebrand.training/en **Simpl!learn** – https://www.simplilearn.com/cyber-security **Koenig SA** – https://koenig-solutionsdl.azurewebsites.net/isaca-information-systems-audit-control-association-training-courses **Enterprise Governance of IT (EGIT)** – https://www.egit.co.za/	https://www.isaca.org/credentialing/cism
		Certified in Risk and Information Systems Control (CRISC)	CRISC recognises accomplishments in developing a well-defined, agile risk management programme based on best practices for identifying, analysing, evaluating, assessing, prioritising and responding to risks. This improves the realisation of benefits and provides the best value to stakeholders.	ISACA	**Firebrand** https://firebrand.training/en **EGIT (Enterprise Governance of IT)** – https://www.egit.co.za/	https://www.isaca.org/credentialing/crisc
		CMIITPSA – Certified Member of IITPSA	The IITPSA's Certified Member distinction ensures that practitioners accepted to this professional designation have the necessary qualifications and demonstrate a sufficient level of relevant professional experience in one or more of the various disciplines that fall under the ICT umbrella. Software, network, or telecommunications engineering, information security, ICT governance, business analysis, database management and administration, ICT lecturing and/or research, project management, business intelligence, software design and/or development, software testing/quality assurance, web development and mobile technologies are just a few examples of such disciplines.	IITPSA	**Deviare** – https://deviare.africa/ **Joburg Centre of Software Engineering (JCSE) –** https://jcse.org.za/ **Mobile Applications Laboratory NPC (Mlab) –** https://mlab.co.za/programmes/ **Regenesys Business School –** https://regenesys.net/	https://www.iitpsa.org.za/certified-member-cmiitpsa/

Water sector cybersecurity considerations	Work roles	Certification	Description	Professional body accrediting certification	Local training vendors	Link
Securing the supply chain	Third Party Cyber Security Officer	Certified Information Security Manager (CISM)	Expertise in information security governance, program development and management, incident management and risk management is demonstrated by certification.	ISACA	**Firebrand** https://firebrand.training/en **Simpl!learn** – https://www.simplilearn.com/cyber-security **Koenig SA** – https://koenig-solutionsdl.azurewebsites.net/isaca-information-systems-audit-control-association-training-courses **Enterprise Governance of IT (EGIT)** – https://www.egit.co.za/	https://www.isaca.org/credentialing/cism
		CMIITPSA – Certified Member of IITPSA	The IITPSA's Certified Member distinction ensures that practitioners accepted to this professional designation have the necessary qualifications and demonstrate a sufficient level of relevant professional experience in one or more of the various disciplines that fall under the ICT umbrella. Software, network, or telecommunications engineering, information security, ICT governance, business analysis, database management and administration, ICT lecturing and/or research, project management, business intelligence, software design and/or development, software testing/quality assurance, web development and mobile technologies are just a few examples of such disciplines.	IITPSA	**Deviare** – https://deviare.africa/ **Joburg Centre of Software Engineering (JCSE)** – https://jcse.org.za/ **Mobile Applications Laboratory NPC (Mlab)** – https://mlab.co.za/programmes/ **Regenesys Business School** – https://regenesys.net/	https://www.iitpsa.org.za/certified-member-cmiitpsa/
Systems acquisition, development and maintenance	1. Warning/Threat Analysis: Threat/Warning Analyst 2. Exploitation Analysis: Exploitation Analyst 3. All-Source Analysis: All-Source Analyst 4. All-Source Analysis: Mission Assessment Specialist 5. Targets: Target Developer 6. Targets: Target Network Analyst 7. Language Analysis: Multi-Disciplined Language Analyst 8. Vulnerability Assessment and Management: Vulnerability Assessment Analyst	Certified Data Privacy Solutions Engineer (CDPSE)	Data scientists/analysts that mine and analyse data for customer insights, as well as IT professionals that create and implement technical privacy solutions	ISACA	**Firebrand** https://firebrand.training/en	https://www.isaca.org/credentialing/certified-data-privacy-solutions-engineer
		CMIITPSA – Certified Member of IITPSA	The IITPSA's Certified Member distinction ensures that practitioners accepted to this professional designation have the necessary qualifications and demonstrate a sufficient level of relevant professional experience in one or more of the various disciplines that fall under the ICT umbrella. Software, network, or telecommunications engineering, information security, ICT governance, business analysis, database management and administration, ICT lecturing and/or research, project management, business intelligence, software design and/or development, software testing/quality assurance, web development and mobile technologies are just a few examples of such disciplines.	IITPSA	**Deviare** – https://deviare.africa/ **Joburg Centre of Software Engineering (JCSE)** – https://jcse.org.za/ **Mobile Applications Laboratory NPC (Mlab)** – https://mlab.co.za/programmes/ **Regenesys Business School** – https://regenesys.net/	https://www.iitpsa.org.za/certified-member-cmiitpsa/

8 RECOMMENDATIONS

Cybersecurity education and awareness is critical for all organisations. An organisation might have strong technical cybersecurity controls in place, but it will not keep the organisation secure if its employees are not cyber secure. Therefore, it is of utmost importance to ensure that all employees, not just technical staff, have at least a basic working knowledge and understanding of cybersecurity principles. Technical staff in key positions requires advanced cybersecurity knowledge which can be obtained via professional certifications and courses.

This document provides a baseline cybersecurity awareness study which should guide organisations in the water sector to improve employees' cybersecurity awareness levels. The survey can assist in determining the baseline cybersecurity awareness of the employees whereafter the training material can be utilised by organisations to guide their employees to improve their levels of cybersecurity awareness.

The main recommendations include:

- Cybersecurity education and awareness should be a continuous process which must be informed by new knowledge as new approaches are used in new cybersecurity incidents.
- To determine the employees' level of cybersecurity awareness, a baseline must be created and then monitored to ensure improvement over time. The baseline can inform the organisation which specific elements need improvement and can then be targeted through organisation wide cybersecurity awareness sessions.
- There exist a wide range of online open-source training material available, which can be use by the organisation and individual employees to improve their cybersecurity awareness.
- Organisations must ensure that they integrate online training with interactive sessions to provide organizational context.
- Organisations should approach cybersecurity awareness training from two levels:
    - Individual: encourage self-learning to improve general cybersecurity awareness.
    - Organisation: conduct organisation wide awareness sessions to address shortcomings in key areas as guided by the baseline cybersecurity awareness survey.
    - Executive / leadership: cybersecurity issues are not purely a technology problem and requires a layered approach to protect organisations, which

includes training, strategy and knowledge regarding the correct reactions to cyber incidents.

- The improvement of cybersecurity awareness in a continuous process which requires regular cybersecurity awareness level measurements, training sessions and monitoring of new incidents and mitigation measures.

This document also provides insight into the cybersecurity work roles which are required in the water sector. Professional certifications and training contained in this document can be used to guide organisations in providing their professionals with professional certifications required in the field of cybersecurity.

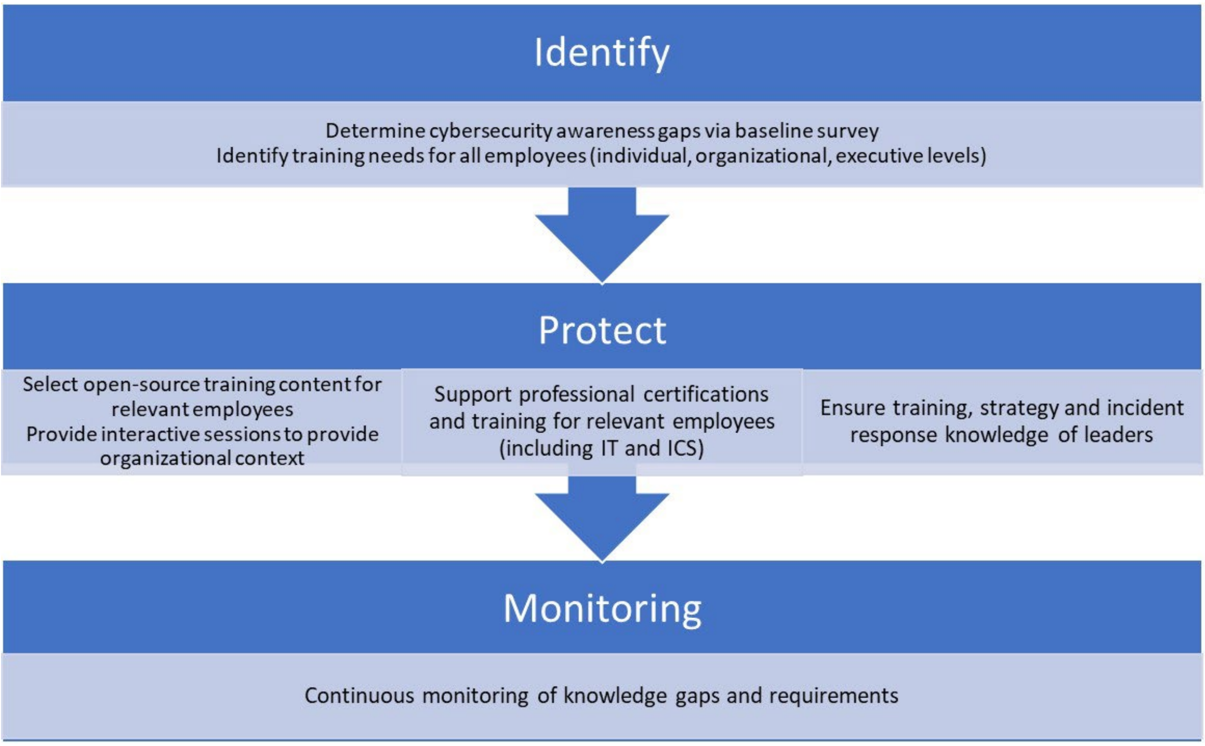
The main recommendations include:

- Organisations must determine the key cybersecurity work roles required in their organisations.
- Organisations can utilise the guidelines presented in this document to develop career paths for technical personnel to obtain professional cybersecurity certifications.
- Professional cybersecurity training and education must be a continuous process which requires regular cybersecurity work role requirement assessments based on organisational needs and industry advancements.

It is important to acknowledge that cybersecurity awareness and training is required by all staff within an organisation, training must be relevant, contextualised and personalized. This means that all employees must receive training which are relevant to their operations, whether that is in a technical or non-technical context, whether operational, support or executive. This document focussed on general cybersecurity awareness as well as professional certification and training, but it must be recognised that executive / leadership training is another level of training which must be considered within an organisation.

Cybersecurity training on an executive / leadership level should include general cybersecurity awareness as high-ranking executives are prime targets for cyber attacks due to their high-level privileges within organisations. However, training should also focus on non-technical issues such as humanistic and managerial aspects of cybersecurity, making risk-based decisions, develop best practices and strategy in cyber resilience.

The following diagram indicates the process which should ideally be followed by organisations to support in the process on becoming more cyber secure.



Identify

Determine cybersecurity awareness gaps via baseline survey
Identify training needs for all employees (individual, organizational, executive levels)

Protect

Select open-source training content for relevant employees
Provide interactive sessions to provide organizational context

Support professional certifications and training for relevant employees (including IT and ICS)

Ensure training, strategy and incident response knowledge of leaders

Monitoring

Continuous monitoring of knowledge gaps and requirements

9 CONCLUSIONS

The report contains two cybersecurity training sets which can help entities in the water sector to improve their general cybersecurity awareness knowledge and to guide them on the professional qualifications which can be pursued by cybersecurity professionals in the water sector.

It is acknowledged that organisational resilience can only be achieved through a layered approach with a combination of technical, formal, and informal mitigation strategies and that cybersecurity knowledge alone will not be sufficient. A fundamental aspect to create a cybersecurity culture of resilience is that employees must be empowered to understand cybersecurity vulnerabilities and the important role that they play in securing themselves and their organisation. This empowerment requires employees to have a certain level of cybersecurity awareness, be engaged in continuous training and communication. Employees in this case includes all employees, both non-technical and technical professionals, support staff and executive / leadership of organisations.

Although a general level of cybersecurity awareness is required by all staff within an organisation, training must be relevant, contextualised and personalized. This means that all employees must receive training which are relevant to their operations, whether that is in a technical or non-technical context, whether operational, support or executive.

REFERENCES

Abazi, B. & Kő, A. (2019). Semi-automated information security risk assessment framework for analyzing enterprises security maturity level. *Lecture Notes in Business Information Processing*. Springer International. doi: 10.1007/978-3-030-37632-1_13

Adams, M. & Makramalla, M. (2015). Paget's disease: Another paramyxovirus in the archaeological record. *Cybersecurity Skills Training: An Attacker-Centric Gamified Approach. Technology Innovation Management Review, 5(1).* https://doi.org/10.15173/nexus.v12i1.150

Agarwal, C. & Singhal, A. (2017). Securing our digital natives: A study of commonly experience [sic] internet safety issues and a one-stop solution. *ACM International Conference Proceeding Series, Part F1280*, pp. 178-186. doi: 10.1145/3047273.3047303

AlMindeel, R. & Martins, J. T. (2021). Information security awareness in a developing country context: Insights from the government sector in Saudi Arabia. *Information Technology and People*, *34*(2), 770-788. https://doi.org/10.1108/ITP-06-2019-0269

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers and Security*, *98*. https://doi.org/10.1016/j.cose.2020.102003

Amjad, H. A. R., Zaffar, M. F., Naeem, U., Choo, K. K. R. & Zaffar, M. A. (2016). Improving security awareness in the government sector. *ACM International Conference Proceeding Series*, 8-10 June, pp. 1-7. doi: 10.1145/2912160.2912186

Ani, P., He, H. & Tiwari, A. (2016). Human capability evaluation approach for cyber security in critical industrial infrastructure. *Advances in Human Factors in Cyebrsecurity*, *501*, 267-277. https://doi.org/10.1007/978-3-319-41932-9

Baltar, F. & Brunet, I. (2012). Social research 2.0: Virtual snowball sampling method using Facebook. *Internet Research*, *22*, 57-74.

Beck, T., Rodina, L., Luker, E. & Harris, L. (2016). *Institutional and policy mapping of the water sector in South Africa*. Cape Town. doi: 10.13140/RG.2.2.32761.88164

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

Bryman, A. & Bell, E. (2011). *Business research methods*. Oxford: Oxford University Press.

Burghouwt, P., Maris, M., Van Peski, S., Luiijf, E., Van de Voorde, I. & Spruit, M. (2017). Cyber targets water management. 11th International Conference on Critical Information Infrastructures Security, 10-12 October, http://resolver.tudelft.nl/uuid:323b1a30-c270-477a-9094-3e6b9f47200d

Campbell, S. G., O'Rourke, P. & Bunting, M. F. (2015). Identifying dimensions of cyber aptitude: The design of the cyber aptitude and talent assessment. *Proceedings of the Human Factors and Ergonomics Society*, pp. 721-725. doi: 10.1177/1541931215591170

Carlton, M., Levy, Y. & Ramim, M. (2019). Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills. *Information and Computer Security*, *27*(1), 101-121. https://doi.org/10.1108/ICS-11-2016-0088

Caulkins, B., Marlowe, T. & Reardon, A. (2019). Cybersecurity skills to address today's threats. *Advances in Intelligent Systems and Computing*, *782*, 187-192. doi: 10.1007/978-3-319-94782-2_18

Chowdhury, N. & Gkioulos, V. (2021). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review*, *40*, 100361. https://doi.org/10.1016/j.cosrev.2021.100361

Cindana, A. & Ruldeviyani, Y. (2019). Measuring information security awareness on employee [sic] using HAIS-Q: Case study at XYZ firm. *2018 International Conference on Advanced Computer Science and Information Systems*, pp. 289-294. doi: 10.1109/ICACSIS.2018.8618219

Clark, R. M., Panguluri, S., Nelson, T. D. & Wyman, R. P. (2016). Protecting drinking water utilities from cyber threats. Idaho: Idaho National Laboratory.

Da Veiga, A. (2016). A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. *Proceedings of 2016 SAI Computing Conference,* 1006-1015. https://doi.org/10.1109/SAI.2016.7556102

Dahlian Persadha, P., Waskita, A. A., Fadhila, M. I., Kamal, A. & Yazid, S. (2016). *How inter-organizational knowledge sharing drives national cyber security awareness: A case study in Indonesia*. *January*, 1-1. https://doi.org/10.1109/icact.2016.7423467

Dawson, M., Taveras, P. & Taylor, D. (2019). Applying software assurance and cybersecurity NICE job tasks through secure software engineering labs. *Procedia Computer Science*, *164*, 301-312. doi: 10.1016/j.procs.2019.12.187

Diamantopoulou, V., Tsohou, A. and Karyda, M. (2020) 'From ISO/IEC 27002:2013 information security controls to personal data protection controls: Guidelines for GDPR compliance', Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 11980 LNCS(July), pp. 238-257. doi: 10.1007/978-3-030-42048-2_16.

Erdogan, G., Romero, A. Á., Zazzeri, N., Žitnik, A., Basile, M., Aprile, G., Osório, M., Pani, C. & Kechaoglou, I. (2021). Developing cyber-risk centric courses and training material for cyber ranges: A systematic approach. *Proceedings of the 7th International Conference on Information Systems Security and Privacy*, *January*, 702-713. https://doi.org/10.5220/0010393107020713

Ficco, M. & Palmieri, F. (2019). Leaf: An open-source cybersecurity training platform for realistic edge-IoT scenarios. *Journal of Systems Architecture*, *97*(September 2018), 107-129. https://doi.org/10.1016/j.sysarc.2019.04.004

Fricker, R. D. & Schonlau, M. (2002). Advantages and disadvantages of internet research surveys: Evidence from the literature. *Field Methods*, *14*, 347-367.

Furnell, S. (2021). The cybersecurity workforce and skills. *Computers and Security*, 100, 102080. doi: 10.1016/j.cose.2020.102080

Gangire, Y., Da Veiga, A. & Herselman, M. (2020). Information security behavior: Development of a measurement instrument based on the self-determination theory. *IFIP Advances in Information and Communication Technology*. Springer International. doi: 10.1007/978-3-030-57404-8_12

Germano, J. H. (2019). *Cybersecurity risk & responsibility in the water sector*. New York: American Water Works Association.

GreenCape. (2014). *Market intelligence report: Water*. Cape Town.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*. https://reader.elsevier.com/reader/sd/pii/S2405844017309982?token=825F4D5FD0127B0A8C8C470FC3E81D1ABB4BC845138F39113801012ACC189AF4CB663406D5E4486B841DB671AD4F3925

Hassanzadeh, A., Rasekh, A., Galelli, S., Aghashahi, M., Taormina, R., Ostfeld, A. & Banks, M. K. (2020). A review of cybersecurity incidents in the water sector. *Journal of Environmental Engineering*, *146*. doi: 10.1061/(asce)ee.1943-7870.0001686

Higgins, J. & Green, S. (2008). Chapter 22: Overview of reviews. Cochrane handbook for systematic reviews of interventions. *Cochrane Database of Systematic Reviews*, 187-235.

Ikhsan, M. G. & Ramli, K. (2019). Measuring the information security awareness level of government employees through phishing assessment. *34th International Technical Conference on Circuits/Systems, Computers and Communications,* pp. 16-19. doi: 10.1109/ITC-CSCC.2019.8793292

International Organization for Standardization. (2013). *ISO/IEC 27002:2013 Information Technology - Security techniques - Code of practice for information security controls*. Geneva: ISO/IEC.

Interpol. (2021). African cyberthreat assessment report: Interpol's key insight into cybercrime in Africa. Lyon.

Jazri, H. & Jat, D. S. (2017). A quick cybersecurity wellness evaluation framework for critical organizations. *Proceedings of 2016 International Conference on ICT in Business, Industry, and Government*. doi: 10.1109/ICTBIG.2016.7892725

Jin, G., Tu, M., Kim, T. H., Heffron, J. & White, J. (2018). Game based cybersecurity training for high school students. *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*, February 2018, 68-73. https://doi.org/10.1145/3159450.3159591

Karampidis, K., Panagiotakis, S., Vasilakis, M., Markakis, E. K. & Papadourakis, G. (2019). Industrial cybersecurity 4.0: Preparing the operational technicians for industry 4.0. *IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks.* https://doi.org/10.1109/CAMAD.2019.8858454

Khan, A. H., Sawhney, P. B., Das, S., & Pandey, D. (2020). SartCyber Security Awareness Measurement Model (APAT). 2020 International Conference on Power Electronics and IoT Applications in Renewable Energy and Its Control, PARC 2020, 298-302. https://doi.org/10.1109/PARC49193.2020.236614

Kour, R. & Karim, R. (2020). Cybersecurity workforce in railway: Its maturity and awareness. *Journal of Quality in Maintenance Engineering*. doi: 10.1108/JQME-07-2020-0059

Kruger, H. A. & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers and Security*, 25(4), 289-296. doi: 10.1016/j.cose.2006.02.008

Lancaster, G. (2005). *Research methods in management: A concise introduction to research in management and business consultancy.* Burlington, MA: Elsevier Butterworth-Heinemann.

Lebek, B., Uffen, J., Neumann, M., Hohler, B. & Breitner, H. M. (2014). Information security awareness and behavior: A theory-based literature review. *Management Research Review*, *37*(12), 1049-1092.

Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gøtzsche, P. C., Ioannidis, J. P. A., Clarke, M., Devereaux, P. J., Kleijnen, J. & Moher, D. (2009). The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: Explanation and elaboration. *Journal of Clinical Epidemiology,* 62. e1-34. 10.1016/j.jclinepi.2009.06.006.

Limba, T., Plėta, T., Agafonov, K. & Damkus, M. (2019). Cyber security management model for critical infrastructure. The International Journal of Entrepreneurship and Sustainability issues 4(4), http://doi.org/10.9770/jesi.2017.4.4(12)

Luiijf, E., Ali, M. and Zielstra, A. (2011). Assessing and improving SCADA security in the Dutch drinking water sector. *International Journal of Critical Infrastructure Protection*, *4*(3-4), 124-134. doi: 10.1016/j.ijcip.2011.08.002

Lusthaus, J., Bruce, M., & Phair, N. (2020). Mapping the geography of cybercrime: A review of indices of digital offending by country. *Proceedings – 5th IEEE European Symposium on Security and Privacy Workshops,* 448-453. https://doi.org/10.1109/EuroSPW51379.2020.00066

Meades, P. (2015). Doing a literature review in health and social care: A practical guide. *British Journal of Guidance & Counselling*. doi: 10.1080/03069885.2014.975101

Mejias, R. J. & Balthazard, P. A. (2014). A model of information security awareness for assessing information security risk for emerging technologies. *Journal of Information Privacy and Security*, *10*(4), 160-185. doi: 10.1080/15536548.2014.974407

Mishra, S., Raj, R. K., Romanowski, C. J., Schneider, J. & Critelli, A. (2015). On building cybersecurity expertise in critical infrastructure protection. *2015 IEEE International Symposium on Technologies for Homeland Security*. https://doi.org/10.1109/THS.2015.7225263

Mohamed Shaffril, H. A., Samsuddin, S. F. & Abu Samah, A. (2020). The ABC of systematic literature review: The basic methodological guidance for beginners. *Quality and Quantity*, 1-28.

Nagarajan, A., Allbeck, J. M., Sood, A. & Janssen, T. L. (2012). Exploring game design for cybersecurity training. *Proceedings – 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems,* 256-262. https://doi.org/10.1109/CYBER.2012.6392562

Nel, N., Swartz, C. D., Moodley N. & Jackson, M. J. (2021). Water Research Development and Innovation Roadmap Skills Mapping Study, Volume 3: Short Course Skills Mapping Study in 2021. WRC Report No. 2305/1/15, Water Research Commission Department of Science and Technology, Department of Water and Sanitation.

Newhouse, W., Keith, S., Scribner, B. and Witte, G. (2017) National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. Gaithersburg, MD. doi: 10.6028/NIST.SP.800-181.

Normandia, Y., Kumaralalita, L., Hidayanto, A. N., Nugroho, W. S. & Shihab, M. R. (2019). Measurement of employee information security awareness using analytic hierarchy process (AHP): A case study of foreign affairs ministry. *Proceedings – 2018 4th International Conference on Computing, Engineering, and Design*, pp. 52-56. doi: 10.1109/ICCED.2018.00020

Nowell, L. S., Norris, J. M., White, D. E. & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods, 16*, 1-13.

Nunes, P., Antunes, M. & Silva, C. (2021). Evaluating cybersecurity attitudes and behaviors in Portuguese healthcare institutions. *Procedia Computer Science*, *181*(2019), 173-181. doi: 10.1016/j.procs.2021.01.118

Öłütçü, G., Testik, Ö. M. & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers and Security*, *56*, 83-93. doi: 10.1016/j.cose.2015.10.002

Panguluri, S., Phillips, W. & Cusimano, J. (2011). Protecting water and wastewater infrastructure from cyber attacks. *Frontiers of Earth Science*, *5*(4), 406-413. doi: 10.1007/s11707-011-0199-5

Park, S.-N. & Park, D.-W. (2018). Cybersecurity system for water treatment SCADA system. *Journal of Engineering and Applied Sciences*, *13*(11), 8712-8715. http://library1.nida.ac.th/termpaper6/sd/2554/19755.pdf

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers and Security*, *66*, 40-51. doi: 10.1016/j.cose.2017.01.004

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers and Security*, *42*, 165-176. doi: 10.1016/j.cose.2013.12.003

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M. & Jerram, C. (2014). A study of information security awareness in Australian government organisations. *Information Management and Computer Security*, *22*(4), 334-345. doi: 10.1108/IMCS-10-2013-0078

Petersen, R., Santos, D., Smith, M. C., Wetzel, K. A. & Witte, G. (2020). Workforce Framework for Cybersecurity (NICE Framework). Gaithersburg, MD. doi: 10.6028/NIST.SP.800-181r1

Prins, S., Marnewick, A. & Von Solms, S. (2020). Cybersecurity awareness in an industrial control systems company. *European Conference on Information Warfare and Security, ECCWS*, 314-323. https://doi.org/10.34190/EWS.20.010

Purssell, E. & McCrae, N. (2020). *How to perform a systematic literature review*. doi: 10.1007/978-3-030-49672-2

Puspitaningrum, E. A., Devani, F. T., Putri, V. Q., Hidayanto, A. N., Solikin & Hapsari, I. C. (2018). Measurement of employee information security awareness: Case study at a government institution. *Proceedings of the 3rd International Conference on Informatics and Computing*. doi: 10.1109/IAC.2018.8780571

Rege, A. (2016). Incorporating the human element in anticipatory and dynamic cyber defense. 2016 IEEE International Conference on Cybercrime and Computer Forensic, ICCCF 2016. https://doi.org/10.1109/ICCCF.2016.7740421

Rege, A., Nguyen, T. & Bleiman, R. (2020). A social engineering awareness and training workshop for STEM students and practitioners. *2020 9th IEEE Integrated STEM Education Conference,* 1-6. https://doi.org/10.1109/ISEC49744.2020.9280596

Ruiters, C. & Matji, M. P. (2015). Water institutions and governance models for the funding, financing and management of water infrastructure in South Africa. *Water SA*, *41*(5), 660-676. doi: 10.4314/wsa.v41i5.09

Saharinen, K., Backlund, J. & Nevala, J. (2020). Assessing cyber security education through NICE cybersecurity workforce framework. *ACM International Conference Proceeding Series*, pp. 172-176. doi: 10.1145/3436756.3437041

Schmeelk, S. & Dragos, D. (2020). Wireless security: Examining the next NICE framework iteration based on industry requirements. *Cybersecurity Skills Journal: Practice and Research*, (Special), 59-73.

Sekaran, U. & Bougie, R. (2016). *Research methods for business: A skills building approach*. 7th ed. New York: John Wiley & Sons.

SFIA Foundation. (2018). *Skills Framework of the Information Age (SFIA): The complete reference*. https://www.sfia-online.org/en

Skiba, R. (2020). Water industry cyber security human resources and training needs. *International Journal of Engineering Management*, *4*(1). doi: 10.11648/j.ijem.20200401.12

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*(August), 333-339. doi: 10.1016/j.jbusres.2019.07.039

South Africa Operational Risk Report. (2021). *Fitch Solutions Risk Reports, 54*(4).

State Security Agency. (2015). The National Cybersecurity Policy Framework for South Africa. www.gpwonline.co.za

Stouffer, K. & Candell, R. (2014). Measuring impact of cybersecurity: On the performance of industrial control systems. *Mechanical Engineering*, *136*(12), 4-7. doi: 10.1115/1.2014-dec-5

Svahnberg, M., Gorschek, T., Feldt, R., Torkar, R., Saleem, S. Bin, & Shafique, M. U. (2010). A systematic review on strategic release planning models. *Information and Software Technology*, *52*(3), 237-248.

The White House. (2013). *Presidential Policy Directive Critical Infrastructure Security and Resilience. Technical report*. Washington DC.

Turkanović, M., Welzer, T. & Hölbl, M. (2019). An example of a cybersecurity education model. *29th Annual Conference of the European Association for Education in Electrical and Information Engineering,* 2019-2022. https://doi.org/10.1109/EAEEIE46886.2019.9000440

Varga, S., Brynielsson, J. & Franke, U. (2018). Information requirements for national level cyber situational awareness. *Proceedings of the 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining,* 774-781. https://doi.org/10.1109/ASONAM.2018.8508410

von, Solms, S. and Marnewick, A. (2018) 'Towards Educational Guidelines for the Security Systems Engineer', in *11th IFIP World Conference on Information Security Education (WISE),* pp. 57-68. doi: 10.1007/978-3-319-99734-6_5ï.

Von Solms, R., & Von Solms, B. (2015). National cyber security in South Africa: A letter to the minister of cyber security. *Proceedings of the 10th International Conference on Cyber Warfare and Security, ICCWS 2015*, 369-374.

Water Information Sharing and Analysis Center. (2019). *15 cybersecurity fundamentals for water and wastewater utilities: Best practices to reduce exploitable weaknesses and attacks*. Washington. www.waterisac.org

Water Sector Coordinating Council Cybersecurity Working Group. (2008). *Roadmap to secure control systems in the water sector*. Washington DC.

Wei, D., Lu, Y., Jafari, M., Skare, P. & Rohde, K. (2010). An integrated security system of protecting smart grid against cyber attacks. *Innovative Smart Grid Technologies Conference*. doi: 10.1109/ISGT.2010.5434767

Xiao, Y. & Watson, M. (2019). Guidance on conducting a systematic literature review. *Journal of Planning Education and Research*, *39*(1), 93-112.

Yost, W. (2019). Water sector cybersecurity risk management guidance. American Water Works Association, White Paper. https://www.awwa.org/Portals/0/AWWA/ETS/Resources/AWWACybersecurityGuidance2019.pdf?ver=2019-09-09-111949-960

Zhang, Z., He, W., Li, W. & Abdous, M. (2021). Cybersecurity awareness training programs: A cost-benefit analysis framework. *Industrial Management and Data Systems*, *121*(3), 613-636. https://doi.org/10.1108/IMDS-08-2020-0462

Zulfia, A., Adawiyah, R., Hidayanto, A. N. & Fitriah Ayuning Budi, N. (2019). Measurement of employee information security awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q): Case study at PT. PQS. *5th International Conference on Computing Engineering and Design*. doi: 10.1109/ICCED46541.2019.9161120

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F. & Basim, H. N. (2020). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, *62*(1), 82-97. doi: 10.1080/08874417.2020.1712269