UNIVERSITY OF JOHANNESBURG

COPYRIGHT AND CITATION CONSIDERATIONS FOR THIS THESIS/ DISSERTATION


- Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.
- NonCommercial — You may not use the material for commercial purposes.
- ShareAlike — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

**How to cite this thesis**

Surname, Initial(s). (2012). Title of the thesis or dissertation (Doctoral Thesis / Master's Dissertation). Johannesburg: University of Johannesburg. Available from: http://hdl.handle.net/102000/0002 (Accessed: 22 August 2017).

# Cybersecurity knowledge requirements for a water sector employee

A Minor Dissertation Submitted in Partial Fulfilment of the Degree of

Master of Philosophy

in

ENGINEERING MANAGEMENT

at the

FACULTY OF ENGINEERING AND THE BUILT ENVIRONMENT

of the

UNIVERSITY of JOHANNESBURG

by

Rendani Thomani (201202458)

Date

11 November 2021

SUPERVISOR: Prof. Annlizé Marnewick

CO-SUPERVISOR: Prof. Suné von Solms, Dr. Masike Malatji

# DECLARATION

I, Rendani Thomani, student number 201202458, hereby declare that the minor dissertation "Cybersecurity knowledge requirements for a water sector employee" submitted for the Master of Philosophy (MPhil) in Engineering Management degree to the University of Johannesburg, apart from the help recognised, is my own work and has not previously been submitted to another university or institution of higher education for a degree.

Signed at Johannesburg, South Africa on the 27th day of October 2021.

Signature _____

UNIVERSITY
OF
JOHANNESBURG

# ABSTRACT

Critical infrastructure in South Africa remains highly vulnerable to cybercrime threats due to a poor cyber-crime fighting capacity and a lack of a strong cybersecurity policy. South Africa appears to have lagged behind in terms of securing and defending cyberspace, despite the country's reliability and its interconnectedness to the Internet. Furthermore, the rapid increase in remote working owing to Covid-19 has raised cybersecurity concerns, the prevalence of cybersecurity assaults and cybercrime has substantially increased, and state organizations have recently been victim to cyber-attacks. Cyber threats can be defined as attempting to gain unauthorized access to infrastructure systems through data communication pathways in an unauthorized manner.

Globally, the water and wastewater sector were ranked number four in the global security incidents based on the Repository of Industrial Security Incidents. To date, systems that can protect themselves without involving human element has not yet been realized, as a consequence, systems are prone to be threatened by random or organized crimes through preying on humans. There is therefore a need to examine internal procedures and protection mechanisms to prevent cyber-attacks. Research shows that humans are the weakest link in cyberspace security as the internet users as well as the only guardian of computers and organizational network.

This research presents the findings of a systematic literature review conducted to assess the cybersecurity knowledge required for a general employee in the water sector. This research further proposes a framework for determining the minimum knowledge required of a general employee in the water sector in order to protect the critical infrastructure. A systematic literature review was adopted from which this research followed the guidelines and procedures from the Cochrane handbook for Systematic Reviews of Interventions.

Following the rigorous process and procedure of the systematic literature review, the final studies chosen for analysis and synthesis amounted to 23 out of the initial collected 2013 studies. Thematic analysis was used to examine the 23 studies. Following the analysis, eight themes for challenges were identified, the blocks of cybersecurity knowledge that employees must have been identified as: 1) Security breaches, 2) Unauthorized access, 3) Negligence, 4) Social Engineering, 5) Malicious insider, 6) Malware/Ransomware, 7) Stolen credentials, and 8) Denial of service.

Furthermore, four themes for mitigating the eight identified cybersecurity challenges were identified as: 1) Cybersecurity knowledge and skills, 2) Cybersecurity awareness, 3) Cybersecurity culture and 4) Cybersecurity training. The first theme (cybersecurity knowledge and skills) assisted in identifying the cybersecurity knowledge required for employees. The second theme (cybersecurity awareness) and the third theme (cybersecurity culture) looked at finding meaning in what organisations can do to urge cybersecurity culture and awareness. Overall, the first, second and third themes assisted in answering the research question. The fourth and last theme focused on identifying the types of general employee cybersecurity training methods that can be undertaken to improve cyber resilience. The identified challenges and the mitigations were further used to develop a model to train employees in cybersecurity, the model will benefit the water sector by identifying key aspects to train employees in order to reduce the intrusion into cyber systems and processes that are used to run and operate critical infrastructure.


UNIVERSITY OF JOHANNESBURG

# ACKNOWLEDGEMENT

First and foremost, I am grateful to the Almighty God for providing me with the strength and wisdom. I would like to thank my family for their patience and support during the journey of my studies.

My appreciation goes to my supervisors, Prof. Annlizé Marnewick, Prof. Suné von Solms and Dr. Masike Malatji for initiating such an interesting project and one that expands the boundaries of engineering by looking at institutional and management issues. I am grateful for all the support, guidance, patience, prompt feedbacks and the enthusiasm for the subject throughout this study.

I would also like to acknowledge the financial support provided by the Water Research Commission (WRC) of South Africa. This research study was funded by the Water Research Commission (WRC) of South Africa, grant number 2021/2023-00354.

UNIVERSITY OF JOHANNESBURG

# TABLE OF CONTENT

DECLARATION ..... ii
ABSTRACT ..... iii
ACKNOWLEDGEMENT ..... iv
TABLE OF CONTENT ..... v
LIST OF FIGURES ..... vii
LIST OF TABLES ..... vii
LIST OF ABBREVIATION ..... viii
Chapter 1: Introduction ..... 9
1.1 Background ..... 9
1.2 Problem statement ..... 10
1.3 Research question ..... 11
1.4 Research objectives ..... 11
1.5 Justification of the study ..... 11
1.6 Research process ..... 12
1.7 Document layout ..... 13
1.8 Conclusion ..... 13
Chapter 2 : Research methodology ..... 14
2.1 Systematic literature review ..... 14
2.2 Systematic review process ..... 15
2.3 Planning the review ..... 17
2.4 Conducting the review ..... 19
2.5 Data analysis and synthesis ..... 22
2.6 Conclusion ..... 24
Chapter 3 : Retrieval of documents ..... 25
3.1 Retrieval of documents per database ..... 25
3.2 Step 1: Studies identification ..... 25
3.3 Step 2: Screening for removing duplicates ..... 25
3.4 Step 3: Screening articles for inclusion based on abstract ..... 26
3.5 Screening for eligibility ..... 29

UNIVERSITY OF JOHANNESBURG

3.6 Quality appraisal ..... 31
3.7 Conclusion ..... 33
Chapter 4 : Analysis and Synthesis ..... 34
4.1 Familiarisation with the data ..... 34
4.2 Generating initial codes ..... 36
4.3 Searching for themes ..... 37
4.4 Reviewing the themes ..... 56
4.5 Reporting ..... 59
4.6 Conclusion ..... 64
Chapter 5 : Conclusion ..... 65
5.1 Introduction ..... 65
5.2 Summary of findings ..... 66
5.3 Future studies ..... 68
References ..... 69
APPENDIX A ..... 74
APPENDIX B ..... 81

UNIVERSITY OF JOHANNESBURG

# LIST OF FIGURES

Figure 1-1: Research process (Xiao & Watson, 2019 ; Mohamed Shaffril et al., 2020)
Figure 2-1: Systematic review phases (Kraus et al., 2020; Xiao & Watson, 2019)
Figure 2-2: PICO model
Figure 2-3: Combining concepts for search sets.
Figure 3-1: PRISMA process flow diagram (Liberati et al., 2009)
Figure 4-1: Percentage of articles per the theme.
Figure 4-2: Percentage of articles per the theme
Figure 4-3: Types of cybersecurity threats per study
Figure 4-4: Methods of building cybersecurity knowledge per study
Figure 4-5: IPO Model for Building Cybersecurity Knowledge
Figure 4-6:Framework for identifying cybersecurity knowledge
Figure 5-1: Framework for identifying cybersecurity knowledge

# LIST OF TABLES

Table 2-1: Key search phrases
Table 2-2: Inclusion criteria (Svahnberg et al., 2010)
Table 2-3: Exclusion criteria (Svahnberg et al., 2010)
Table 2-4: Quality appraisal questions (Panchal & Damodaran, 2017).
Table 2-5: Phases of thematic analysis (Braun & Clarke, 2006b)
Table 3-1:Summary of the total retrieved document titles.
Table 3-2: Summary of remaining distinctive document titles after removing duplicates
Table 3-3: Summary of the 55 keywords codes.
Table 3-4: Summary of documents with more than 25 keywords appearances in their abstract
Table 3-5: Studies resulting from reading abstracts
Table 3-6: Included studies
Table 3-7: Excluded studies
Table 3-8: Quality assessment
Table 4-1: Analysis of journal articles
Table 4-2: Analysis of conference papers
Table 4-3: Initial codes
Table 4-4: Summary of generated themes
Table 4-5: Supporting codes for security breaches
Table 4-6: Supporting codes for unauthorised access
Table 4-7: Supporting codes for negligence
Table 4-8: Supporting codes for social engineering
Table 4-9: Supporting codes for malicious insider
Table 4-10: Supporting codes for ransomware/malware
Table 4-11: Supporting codes for stolen credentials
Table 4-12: Supporting codes for denial of service
Table 4-13: Cybersecurity skills and knowledge supporting codes

UNIVERSITY OF JOHANNESBURG

Table 4-14: Cybersecurity awareness supporting themes and codes
Table 4-15: Cybersecurity culture supporting codes
Table 4-16: Cybersecurity training supporting codes
Table 4-17: Summary themes for cybersecurity challenges and frequency of codes
Table 4-18: Summary of themes and frequency of codes

# LIST OF ABBREVIATION

| ACRONYM | DESCRIPTION |
|---|---|
| CASP | Critical Appraisal Skills Program |
| CDSR | Cochrane Database of systematic Reviews |
| CI | Critical Infrastructure |
| CRD | Centre for Research and Dissemination |
| DARE | Database of Abstract of Reviews of Effects |
| ICS | Industrial Control Systems |
| IoT | Internet of Things |
| IPO | Input Process Output |
| IT | Information Technology |
| PICO | Population, Intervention, Comparison Outcome |
| PRISMA | Preferred Reporting Items for Systematic Reviews and Meta-analysis |
| SA | South Africa |
| SCADA | Supervisory Control and Data Acquisition |
| SLR | Systematic Literature Review |
| UK | United Kingdom |
| USA | United States of America |
| NIST | National Institute of Standards and Technology |

UNIVERSITY OF JOHANNESBURG

# Chapter 1: Introduction

## 1.1 Background

In 2009, former state president Jacob Zuma announced that intensifying efforts against identity theft and cybercrime are one of the key initiatives for South Africa, citing the importance of cyber security research (Parker & Brown, 2019). According to Von Solms and Von Solms (2015), South Africa appears to have fallen behind in securing and protecting cyberspace, considering the country's dependability as well as the interconnectedness to the internet.

The rapid rise in remote working due to Covid-19 has increased risks to cybersecurity environments, the prevalence of cybersecurity attacks and cybercrime has significantly increased with state organisations having been recently targeted ("South Africa Operational Risk Report," 2021). In 2020, South Africa was identified as one of the most targeted countries by cyber criminals (Lusthaus et al., 2020) as a consequence the country was ranked first out of the 13 Southern African states and 73rd globally for scoring as high as 61.1% on financial crime and cybercrime. This comes as a result of the lack of a strong cybersecurity policy and poor cybercrime-fighting capacity which means that the critical infrastructure in South Africa remains highly vulnerable to cybercrime threats ("South Africa Operational Risk Report," 2021). Providing, regulating and maintaining national security forms part of government responsibility (Van Vuuren et al., 2013), as such a National Cybersecurity Policy Framework was introduced by the South African government on the 23rd of September 2015. Later in 2019 the government also introduced the Critical Infrastructure Protect Act which was then followed by the Cybercrimes Act that was assented in the 1st June 2021.

Physical processes in water systems have been integrated with computational capabilities, moving towards smart water systems that support real-time decision making to improve efficiency and reliability (Lee et al., 2020).Modern business processes rely on information and information systems to meet the strategic interest of organisations(Alshaikh, 2020a), these systems carry risks such as cyber-related attacks, data theft, financial loss, private information exposure and sabotage (Prins et al., 2020).

Alshaikh (2020) further stated that cybersecurity attacks may result in catastrophic consequences that include leakage of trade secrets and intellectual property or the disruption of mission-critical systems. According to a study by Willis Towers Watson (2019), human error and behaviour contributed an estimate of 90% in cyber-related claims, this makes humans the weakest link in cyberspace security as the internet users as well as the only guardian of computers and organisational networks (World et al., 2016).The water sector is faced with the risk of cyberattacks that may lead to the disruption of a critical operation or a business process this includes theft of customer billing data, controlling pumps or valves and injecting chemicals above the required limits (Shapira et al., 2021)

Cyber threats can be defined as attempting to gain unauthorized access to infrastructure systems through data communication pathways in an unauthorized manner (Panguluri, Phillips, & Cusimano, 2011). Awareness of the vulnerability to manmade and natural threats that exist in the urban water systems has been growing considering droughts, earthquakes, physical and cyber-attacks (Clark et al., 2011). Organizations such as national departments and local municipalities perform tasks such as water management that include controlling water

levels for protecting land from flooding and the purification of wastewater as well as sewage before depositing to the receiving water bodies. These organizations make use of information and communication technologies to fulfil their tasks. They make use of facilities that ranges from standard office Information Technology (IT) to Industrial Control Systems (ICS), as a result of using technology, security-related incidents have increased in recent years in the Industrial Control Systems including the critical infrastructure sectors, this has resulted in the increased cyber risk. There is therefore a need to examine internal procedures and protection mechanisms to prevent cyber-attacks (Burghouwt et al., 2017).

Addressing the protection of the water sector's critical cyber infrastructure is of crucial importance for any country's economy (Malatji et al., 2021). South Africa, like many other countries, has an overarching national cybersecurity strategy aimed at combating cyber terrorism, cybercrime, cyber vandalism, and cyber sabotage (Malatji et al., 2021). Globally, the water and wastewater sector was ranked number four in the global security incidents based on the Repository of Industrial Security Incidents (RISI) that reports on trends affecting industrial control systems and cybersecurity incidents (Panguluri, Phillips, & Cusimano, 2011). The vast majority of points of entry for the attackers occurred via local business networks through remote access. The resultant economic impact due to security incidents indicated that 29% of incidents resulted in damages of more than one million dollars per incident (Panguluri, Phillips, & Cusimano, 2011). The South African economy losses about an estimated ZAR2.2bn as a result of cybercrime ("South Africa Operational Risk Report," 2021).

Higher levels of cyber-attacks and threats are being experienced by many organizations as a result of improved technology and connectivity (Parker & Brown, 2019). According to Bode (2015), systems that can protect themselves without involving human has not yet been realized, as a consequence, systems are prone to be threatened by random or organised cyber-attacks. Fostering of 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, 2020a). This comes after recent security reports pointing out employee noncompliance with organisational information security policies, which has resulted in a significant portion of cybersecurity breaches (Alshaikh, 2020a). There is a shortage in skills and requirements in South Africa for cybersecurity professionals that can safeguard organizations from cybercrime and other cyber-related threats(Parker & Brown, 2019).

## 1.2 Problem statement

Infrastructure, such as water infrastructure, is faced with the problem of being exposed to cyber-attacks when the employees do not have adequate knowledge of cybersecurity. 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 cyber-attacks that might harm service delivery and the overall strategic objectives of the water services authorities. It is therefore important that the employees in the water sector are cyber aware. The resulting problem statement is as follows:

> ***"As one of the critical infrastructures, the water sector is at an increased risk of vulnerability if the employees have inadequate levels of sector-specific cybersecurity awareness".***

Questions aimed at developing possible solutions to the problem stated are illustrated in the following section.

## 1.3 Research question

The research question aims to define the framework to identify the cybersecurity knowledge required for a general employee in the water sector. The objective is to address the following question:

> *What knowledge is essential for employees to urge cybersecurity culture and awareness in the water sector's critical infrastructures*

## 1.4 Research objectives

The objective of this research is to conduct a systematic literature review in the water sector to develop approaches to follow in building the cybersecurity knowledge and awareness for a typical employee, to urge cybersecurity culture within organizations in the water sector. The focus of this research is on protecting the critical water infrastructure against sector-specific cybersecurity attacks. This will be done through the systematic literature review, collecting, and analysing the results that will be generated from the research articles, papers, reports, and books to determine the essential knowledge required for a general employee in the water sector. It is through this process that the research will be able to provide a critical and unbiased outcome.

This research work will benefit the employees in the water sector. This study will form part of a larger project related to the development of cybersecurity education and awareness in the water sector within South Africa, it will become part of the formation of the literature basis which will be used towards the development of educational cybersecurity content to be developed for the South African water sector.

This work will also form the basis for future work which will include the improvement of the theoretical framework through inputs from experts in the water sector. The finalised framework will inform the development of educational material that will educate employees in the sector to better protect the infrastructure and create a cybersecurity culture in the sector.

UNIVERSITY OF JOHANNESBURG

## 1.5 Justification of the study

Reducing the effects of existing and future attacks on smart Critical Infrastructure (CI) is important. Defence techniques have been used to mitigate the effects of cyber-attacks through intrusion detection methods and intrusion prevention methods (Da¸s & Gündüz, 2019). Although such methods are in place, law enforcement has found few answers to cybercrimes, it is only a matter of time before more cyber-attacks on critical infrastructure begin to be experienced (Geers, 2009).

According to Flaus (2019), the lack of awareness of risks associated with cyber-attacks is one of the human factors on the checklist for examining the vulnerabilities of industrial systems. Flaus (2019) further states that many users do not take precautions even though most attacks on industrial sites are through social engineering. Humans are considered to be a problem in the cybersecurity area, considerations must be made to realize the need for mindset change (Zimmermann & Renaud, 2019) that can result in the prevention of data breaches which can be achieved through providing regular cybersecurity awareness training to personnel (He et al., 2019).

## 1.6 Research process

This research will be conducted by making use of a systematic literature review method to review journal articles as well as existing literature to answer the research question and subsequently create a foundation for further research. To provide convincing evidence and to ensure credibility and avoid biases in this research work the systematic literature review method was identified to be a suitable method, based on the fact that the procedure of a systematic literature review enables readers to replicate or build on the search process and get directed to the same or similar direction of the body of research.

The study will follow guidelines from Higgins & Green (2008) supplemented by two articles from Xiao and Watson (2019) and Mohamed Shaffril (2020). From the three sources, a systematic literature review process suitable for this research work was derived into a three-phased approach. Xiao and Watson (2019) indicated that these three major phases must be involved to generate a successful literature review. The following procedure was developed by combining different approaches from Xiao and Watson (2019) and Mohamed Shaffril (2020). The systematic research process is summarised as follows:

- **Phase one:** planning the review will consist of two stages, the first step will be the identification of the need for a review followed by the development of the review protocol.
- **Phase two:** conducting the review will consist of five stages. The first stage will be the identification of research followed by selection of primary studies, study quality assessment, data extraction and data synthesis.
- **Phase three:** reporting the review and data demonstration.

The derived systematic literature review model is followed in this research is illustrated and summarised in Figure 1-1 below.


**Figure 1-1: Research process** (Xiao & Watson, 2019 ; Mohamed Shaffril et al., 2020)

## 1.7 Document layout

Chapter 1 Pertains to the introduction and the proposal and gives an overview of the whole project.

Chapter 2 This chapter discusses the methodology that will be followed to research to meet the objectives of the research.

Chapter 3 Relevant articles will be retrieved following the systematic literature review method. The results will be documented and reported.

Chapter 4 Retrieved articles will be analysed and synthesised using thematic analysis.

Chapter 5 The final chapter summarized the findings and addressed the research question.

## 1.8 Conclusion

In recent years physical processes in water systems have been integrated with computational and physical capabilities, moving towards smart water systems. This comes with risks of cyber-related attacks that come as a result of a shortage in skills and requirements for cybersecurity professionals that can protect organizations from cybercrime. The water sector becomes vulnerable if the employees in the sector do not have adequate knowledge of cybersecurity. As one of the critical infrastructures, the water infrastructure must be protected from cyber-attacks that can harm service delivery. This research will venture into identifying the cybersecurity knowledge required for a general employee in the water sector through answering the research questions, one question being the identification of knowledge required to create a cybersecurity culture while the other is on the approach to follow to build knowledge and awareness.

UNIVERSITY OF JOHANNESBURG

# Chapter 2 : Research methodology

The selected research methodology and the search processes developed will be presented, this will be supported by the rationale behind the selection of specific research methods over other methods available. The developed search process includes planning for the review, conducting and reporting the review.

## 2.1 Systematic literature review

A systematic literature review is used to comprehensively identify up-to-date literature and to synthesize related literature through replicable procedures, organised and transparent (Mohamed Shaffril et al., 2020) to enhance reliability, quality, validity and replicability of the review, tailored to answer the research question(Xiao & Watson, 2019). Systematic literature reviews stress transparency through defined and justified strategies to include and or exclude articles, the reason behind excluding articles must be provided. Adequate information and details must be provided to enable future researchers to replicate the procedures in their studies(Mohamed Shaffril et al., 2020). Furthermore, systematic literature reviews are valuable for planning practitioners that seek evidence to guide their decisions, this means that the quality of evidence can have real-world implications(Xiao & Watson, 2019).

The identification of knowledge gaps and existing inconsistencies in research can be used to benchmark future research to contribute towards understanding a specific topic (Keupp et al., 2012). In essence, systematic literature reviews are methods of interpreting large volumes of data to explain “what works” and “what does not work” (Wood, 2003). The purpose of a systematic review is to gather evidence base in line with the research theme to achieve the overall goal of creating credible policy, research, or practical recommendations (Wood, 2003). Key features of a systematic review include; clearly stated objectives with explicit, reproducible methodology, identification of all possible studies that meet the eligibility criteria, assessing the validity of findings of the included studies using methods such as the risk of bias the last feature is the presentation and synthesis of the characteristics as well as findings of the studies included (Liberati et al., 2009).

UNIVERSITY OF JOHANNESBURG

Systematic literature reviews are used to draw conclusions and thoughts with certainty, consistency and confidence about current knowledge and unknows about the answer to the research question (Briner & Denyer, 2012). Systematic reviews are more fit than traditional reviews in answering a specified question and testing the hypothesis (Petticrew & Roberts, 2008). Although single studies do provide important findings and results, they do come with methodological shortcomings or biases or reach conflicting conclusions by the author (Petticrew & Roberts, 2008), (Centre for Reviews and Dissemination, 2009) thus making systematic literature reviews favourable (Taylor, 2012). As part of evidence based-movement, systematic reviews provide the best available evidence (Boell & Cecez-Kecmanovic, 2015).

To determine the cybersecurity knowledge and awareness for a typical employee to urge cybersecurity culture within organizations in the water sector, there is a need to draw existing knowledge and evidence to inform decisions in concluding in a certain, consistent, and confident manner on what is known and what is not known about the answer to the review question. To ensure evidence-based decision making to emerging problems, systematic literature reviews fulfils the need to access evidence of high quality and reliability in a timeous manner, the reviewing of this evidence leads to an informed system and policy response (Ganann et al., 2010), (Haddaway et al., 2015). To answer the research question, this research requires the gathering of existing peer-reviewed

research work on sector-specific cybersecurity knowledge and awareness (Petticrew & Roberts, 2008).By making use of the systematic review method in this research, the process of selecting studies that meet specific criteria with a sound judgement in confirming the rigour of the evidence produced through previously published studies will be achieved (Ham-baloyi & Jordan, 2015), which will subsequently assist in answering the research question.

This research seeks to determine the cybersecurity knowledge and awareness required for a typical employee in the water sector to urge cybersecurity culture within organizations to decrease vulnerability to cyberattacks. To derive cybersecurity knowledge and awareness for the water sector, the research seeks to firstly accumulate evidence that the problem exists before determining the knowledge and awareness requirements well as current cybersecurity culture within organisations, aimed at developing a deep understanding of existing knowledge (Briner & Denyer, 2012), before identifying the knowledge and awareness that a typical employee in the water sector must have to urge cybersecurity culture. To answer the research question adequately and to achieve the objective of the research, this research requires a method that will make it possible to adequately search relevant literature rigorously and transparently (Liberati et al., 2009)to identify, evaluate and interpret all the available quality relevant literature, particular to the research question (Kitchenham, 2004). A systematic literature review was identified as the most suitable and favourable method (Taylor, 2012) to respond to the research question for this research.

## 2.2 Systematic review process

A systematic review process involves a few steps of discrete activities. The activities have been suggested in different orders in guidelines such as Cochrane Handbook, National Institute of Health and Centre for Research and Dissemination (CRD) (Kitchenham, 2004). This research will follow three rigorous phases that include planning review, conducting the review, and reporting the review. Figure 2-1 below illustrate the review process.

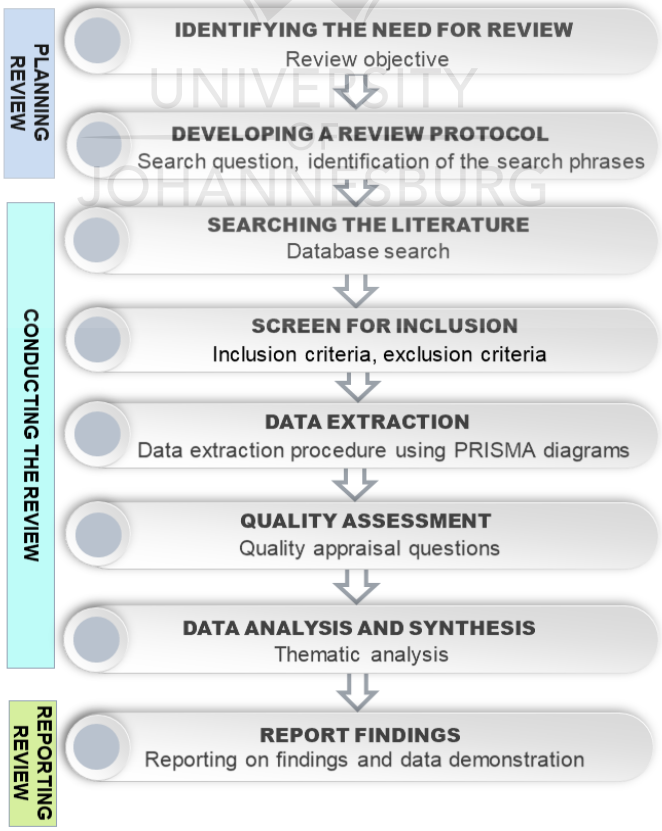


**Figure 2-1: Systematic review phases** (Kraus et al., 2020 ; Xiao & Watson, 2019)

**Identification of the need for a review:** The necessity for this systematic literature review comes as a result of the requirement to gather and summarise the existing literature on cybersecurity knowledge and culture in the water sector in a thorough and unbiased manner (Kitchenham, 2004). The literature review will be driven by the research question through which the selection of studies, the methodology for extracting, synthesis and reporting data thereof will be aimed towards answering the research question (Xiao & Watson, 2019). The aim is to achieve a broader and more general conclusion on the subject matter based on various studies. This will enable the answering of the research question (Kitchenham, 2004).

**Development of the review protocol:** The review protocol is a blueprint that specifies the methodology to be used to conduct a rigorous systematic review (Xiao & Watson, 2019). The preparation of a protocol is in the systematic review process is considered essential, it ensures planning and explicit documenting before starting with the review (Kamioka, 2019). The review protocol development step will define the methods to be used for undertaking the systematic literature review. This will focus on the rationale for the review, research question, search strategy including search terms, resources to be searched and the databases, selection criteria for inclusion and exclusion, quality assessment checklist and procedures, data extraction strategy and the synthesis of the extracted data (Tawfik et al., 2019).

**Searching the literature:** Electronic databases will be used to identify research through the use of keywords that will be derived from the research question. The literature collected for the review will influence the quality of the literature review (Xiao & Watson, 2019). The identification of comprehensive studies relating to the research question will be retrieved through the development of a search strategy that will include searching using various combinations from the research question by breaking down the question into components using population, intervention, comparison, and outcome (PICO) (Tawfik et al., 2019). Search strings will be developed using Boolean AND's and OR's (Xiao & Watson, 2019)

UNIVERSITY OF JOHANNESBURG

**Screening for Inclusion:** The Preferred Reporting Items for Systematic Reviews and Meta-analysis (PRISMA) approach will be followed as suggested by Tawfik (2019) and Mohamed Shaffril (2020) to derive the data set for this research. The four main steps that will be followed in the PRISMA process will be (i) retrieving of studies through searching from the databases followed by (ii) selection of studies through the application of the inclusion criteria before (iii) evaluating the quality of studies through coding and lastly will be the (iv) synthesis where results will be analysed.

**Study quality assessment:** Quality assessment is the important step in the systematic review process for assessing the quality of the primary studies. This step provides more details on the quality appraisal criteria that will be based on the Critical Appraisal Skills Program (CASP). Documents that will be certified to be of the required quality will be used for analysing, interpreting, and concluding the research (Kitchenham, 2004).

**Data extraction:** The included full-text articles will be extracted based on the inclusion criteria and making use of the PRISMA approach. In assessing the quality of the studies, bias will be reduced by adding a data extraction form before the inclusion for the analysis (Tawfik et al., 2019).

**Data analysis and synthesis:** The next step is the interpretation, analysis and synthesis of the data using critical interpretative synthesis (Mohamed Shaffril et al.,2020). This will include collating and summarising the results of

the included primary studies through making use of the descriptive approach where similarities and differences in study outcomes will be highlighted (Kitchenham, 2004) this will be used to answer the research question in the next chapter.

**Reporting findings:** The final step is the reporting of systematic literature reviews. This must be reported in sufficient detail to ensure that the review is reliable and independently repeatable (Xiao & Watson, 2019), Communicating systematic literature review results effectively through communication is important (Kitchenham, 2004).

## 2.3 Planning the review

### 2.3.1 Identification of the need for a review

The objective of the systematic review in this research is to enable the answering of the research question as to; *what knowledge is essential for typical employees in the water sector to urge cybersecurity culture within the organization.* The necessity for this systematic literature review comes as a result of the need to gather and summarise all the existing literature that will present evidence on existing and anticipated sector-specific cybersecurity awareness, where subsequently the knowledge and capabilities required to curb these cybersecurity related attacks will be outlined with the overall goal to create cybersecurity awareness and urge cybersecurity culture in organisations within the water sector. To carry out this task in a rigorous, thorough, and unbiased manner, a systematic literature review was identified as the suitable method.

### 2.3.2 Development of the review protocol

#### 2.3.2.1 Research question

The formulation of the research question is an important task in the development of a protocol (Centre for Reviews and Dissemination, 2009). The research question must be specific on the type of population, intervention, comparison, and outcome (PICO) of interest in the study (Green, 2008). The research question will be structured and framed in terms of PICO to formulate a combination of keywords to be used in the electronic database. Key words identified from the research question using the PICO model is illustrated below:

**RQ:** *What knowledge is essential for employees to urge cybersecurity culture and awareness in the water sector's critical infrastructures?*

From the research question above the PICO acronym was applied to as illustrated in Figure 2-2 below.

UNIVERSITY OF JOHANNESBURG

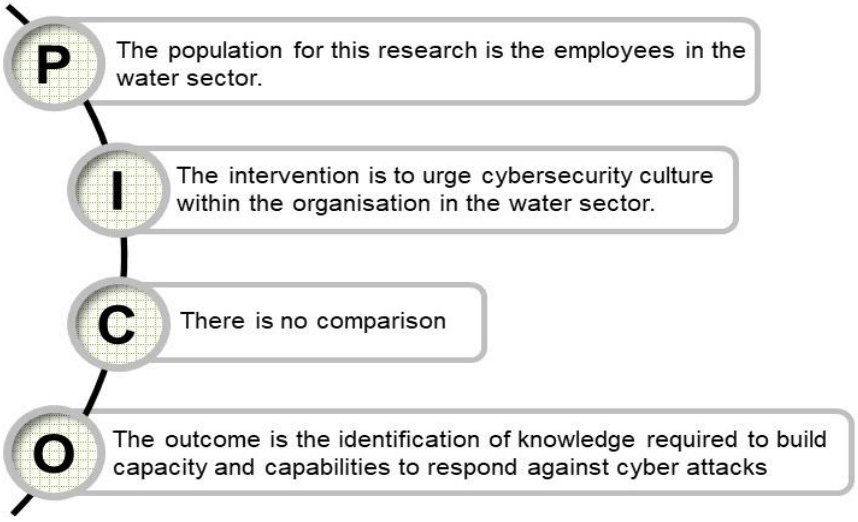


**Figure 2-2: PICO model**

From the above-defined question broken down using PICO, keywords will be identified to assist with focusing the research through the formulation of key search phrases. Since there is no comparison to be undertaken in this research, the modified PICO model will be used.

### 2.3.2.2 Identification of the search phrases

The acquisition of primary studies is one of the aims of the systematic literature review. Studies will be obtained from different databases using the search strategy. The rigour of the search process is what distinguishes systematic reviews from traditional reviews (Kitchenham, 2004). The search strategy must be unbiased to identify as many studies and literature as possible related to the research question.

Key search phrases will be generated using the modified PICO model. Through the search phrases, significant studies and literature related to the research question will be gathered and obtained for the research. Trial searches will be conducted using various combinations of search items derived from the research question. Table 2-1 below is the list of key phrases.

UNIVERSITY OF JOHANNESBURG

**Table 2-1: Key search phrases**

| POPULATION | INTERVENTION | OUTCOME |
|---|---|---|
| Employees | Urge cybersecurity culture | Identify current cybersecurity knowledge |
| | Urge cybersecurity awareness | Identify cybersecurity education and training required |

The search strategy for the research will make use of Boolean operations to build up controlled vocabulary terms for acquiring articles through joining together terms from Table 2-1 with the Boolean “OR” operator. Boolean operations also allow the joining of three terms together with the ‘AND” operator. Figure below illustrate the Boolean operation.

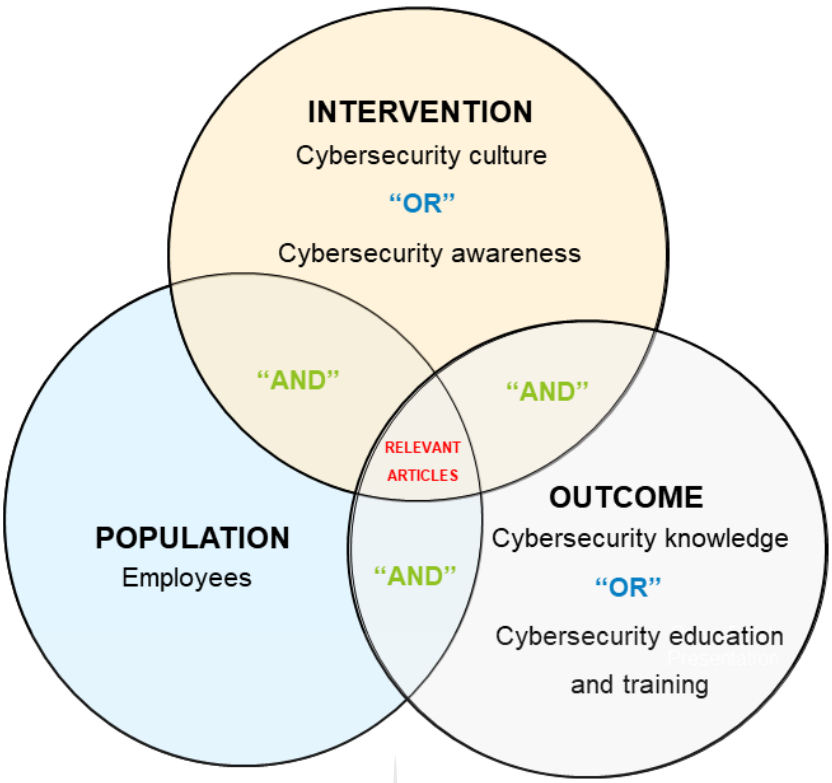


**Figure 2-3: Combining concepts for search sets.**

Following the Boolean operation, search strings may be formulated as follows:

***String 1:*** Employees ***AND*** Cybersecurity *culture* ***AND*** *Cybersecurity knowledge* ***AND*** *Critical Infrastructure*

***String 2:*** Employees ***AND*** Cybersecurity *awareness* ***AND*** *Cybersecurity education and training* ***AND*** *Critical Infrastructure*

## 2.4 Conducting the review

### 2.4.1 Searching the literature

Insightful peer-reviewed studies will be gathered from a selected list of databases. These include peer-reviewed articles, papers, books, and other modified works. Databases in the domain of cybersecurity awareness and knowledge in the water sector will include:

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

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

### 2.4.2 Screening for inclusion

The study selection criteria will be used to identify studies that will provide evidence about the research question to reduce the likelihood of bias. The inclusion/exclusion criterion will be defined for including studies and further selecting the most related studies. The inclusion criteria are prepared for identifying studies that are related to research questions (Svahnberg et al., 2010).

Table 2-2 and Table 2-3 below illustrate the detailed inclusion and exclusion criteria. This will be applied to the studies identified in the inclusion criteria.

**Table 2-2: Inclusion criteria** (Svahnberg et al., 2010)

| **STUDY INCLUSION CRITERIA** | |
|---|---|
| Language in article | Articles delivered in English will be used to avoid tempering with the output quality. |
| Article is peer-reviewed | To ensure the quality of the study, only peer-reviewed studies will be used. |
| Article is in full text | Only full-text articles will be included to accommodate comprehensive reading. |
| Type of article | The article can be comparative, action research, case study, survey, emphatical study |
| Article relation | The article is related to cybersecurity knowledge and awareness in the water sector |
| Article discussion | Articles discuss cybersecurity knowledge requirements for creating awareness |
| Article Evaluation and analysis | The article evaluates and analyses existing cybersecurity knowledge of employees in the water sector |

UNIVERSITY OF JOHANNESBURG

**Table 2-3: Exclusion criteria** (Svahnberg et al., 2010)

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

### 2.4.3 Data extraction

Data extraction is referred to as the most challenging aspect of the systematic literature review methodology given that the process involves going back to primary articles and highlighting the relevant information that will eventually answer the research question (Josette Bettany-Saltikov, 2012). To ensure a transparent and complete reporting of the systematic review and meta-analysis (Liberati et al., 2009), PRISMA diagrams will be used for summarising aggregate data from the identified databases.

PRISMA will present the databases used, records identified through database searching, records remaining after duplicates have been removed, records screened, full-text articles assessed for eligibility, and the studies included for qualitative synthesis. The study selection criteria will follow a stepped approach as illustrated by Liberati (2009). Steps to be followed will include.

**Step 1: Studies Identification,** this step is aimed at searching the database by applying search keys derived from the search strategy. The number of records identified will be recorded.
**Step 2: Screening for removing duplicates**, the number of total records identified will be extracted. After duplicates have been removed.
**Step 3: Screening articles for inclusion based on abstract,** this step is aimed at the screening by applying the inclusion and exclusion criteria. The number of records screened, and records excluded will be quantified.
**Step 4: Screening articles for eligibility,** this step is aimed at screening full-text articles for eligibility by applying the inclusion and exclusion criteria. The number of records screened, and records excluded with reasons for exclusion will be quantified.
**Step 5: Included studies for qualitative synthesis**, The Included studies for qualitative synthesis are quantified will be outlined.

A summary diagram indicating the retrieved and excluded journals/studies will be populated in Chapter 3.

UNIVERSITY OF JOHANNESBURG

### 2.4.4 Quality assessment

According to Kitchenham (2004) study quality relates to the extent to which the study minimises bias and maximises internal and external validity. The study quality assessment will be used to identify various other boundaries that might be overlooked in the study selection criteria. The study quality assessment will assist in investigating whether quality differences explain differences in the study results. This will be achieved through formulating questions to model the study quality assessment. The quality assessment model was adopted from Kitchenham (2004).

Study quality appraisal will be conducted in two stages. The first stage will be reading the article's summary or abstracts and conclusion in each study to assess relevancy. The second stage will be quality appraisal through the 10 CASP checklist of questioning, this will provide for distinguishing issues in a systematic manner (Panchal & Damodaran, 2017).Table 2-4 below outlines the list of the 10 CASP checklist questions.

**Table 2-4: Quality appraisal questions** (Panchal & Damodaran, 2017)**.**

| QUESTIONS FOR STUDY QUALITY ASSESSMENT | |
|---|---|
| Q1 | Is there a clear statement of the aims of this research? |
| Q2 | Is there an appropriate research methodology? |
| Q3 | Is there an appropriate research design in the article that addresses the aims of the research? |
| Q4 | Is there an appropriate data selection strategy in line with the aims of the research? |
| Q5 | Does the data collection address the research issue appropriately? |
| Q6 | Are there adequate considerations of the relationship between the researcher and participants? |
| Q7 | Are there considerations on ethical issues that have been put in place? |
| Q8 | Is there a sufficiently rigorous data analysis? |
| Q9 | Is there a clear statement of findings? |
| Q10 | How valuable is the research? |

## 2.5 Data analysis and synthesis

In this section the research attempt to find the solution to answer the research question. This phase involves assessing the contributions of the studies to answering the review question (Petticrew & Roberts, 2008). The research will try to achieve this by synthesizing evidence from this qualitative research work. The process of data synthesis involves collating and summarising the results of the included primary studies to create a new understanding through comparing and analysing concepts and findings from the different sources that focused on the same topic of interest. Data synthesis requires transparency in the formulation process and requires authors to identify and extract evidence from the studies included to develop combined synthesized findings (Noyes et al., 2008).

UNIVERSITY OF JOHANNESBURG

Providing a robust synthesis of studies is one of the values of the systematic review process. Results can be presented in a form of textual descriptions, a grouping of similar data, transforming data into a common rubric or making use of charts which includes histograms, pie-chart or translating data either by thematic or content analysis (Josette Bettany-Saltikov, 2012).This research will make use of thematic analysing as the preferred method of presenting the synthesized findings of the research work.

### 2.5.1 Thematic analysis

Thematic analysis is defined as the method of identifying, analysing and reporting data patterns(Braun & Clarke, 2006b). Thematic analysis is a process for searching for themes that emerge as being important to the description of the phenomenon (Fereday, 2006). This process starts through the researcher noticing and looking for patterns and issues of potential interest in the data set, this can be during data collection. The analysis involves constant back and forth movement between the data set, the coded extract and the analysis of the data being produced. The thematic analysis to be applied will follow a top-down deductive approach. The existing theoretical concepts will be used to provide a foundation to develop themes (Terry et al., 2021). Below are the concepts and ideas brought to the data in a form of a deductive approach (Braun & Clarke, 2012).

- Employee mindset and behaviour
- Employee awareness and knowledge gaps
- Skills and training requirement
- Organisational culture

Table 2-5 below illustrate the phases that will be followed in conducting thematic analysis (Braun & Clarke, 2006b).

**Table 2-5: Phases of thematic analysis** (Braun & Clarke, 2006b)

| Phases | | Process Description |
|---|---|---|
| 1 | Familiarisation with data | Noting initial ideas, transcribing data, reading data |
| 2 | Generating initial codes | Coding interesting features in the entire data set and collating relevant data |
| 3 | Searching for themes | Collating codes into potential themes and gathering relevant data |
| 4 | Reviewing themes | Verifying if the theme works with the coded extracts in levels 1 and 2 |
| 5 | Define and name themes | Analyse and refine specifics for each theme, outcomes and define themes |
| 6 | Reporting | Final analysis of selected extracts relating to the analysis of the RQ |

**Phase 1: Familiarisation with the data**, Terry considers this first phase the bedrock doing good thematic analysis. The researcher immerses in the data through reading and rereading textual data(Braun & Clarke, 2012). Familiarisation provides the researcher with a point of entry in doing the analysis, in this phase, the researcher generates very early and provisional analytic ideas(Terry et al., 2021). Reflective and theoretical thoughts can be developed through immersion in the data, including interest, values and insights that have grown about the topic (Noyes et al., 2008).

UNIVERSITY OF JOHANNESBURG

**Phase 2: Generating initial codes,** In this second phase the researcher has read the data and has ideas about what is in the data and the interesting points, the initial production of codes takes place where these codes assist the researcher to simplify and focus on specific characteristics of the data (Noyes et al., 2008). Codes are considered building blocks of analysis, data that is potentially relevant to the research question is labelled and identified through the process of coding which can be done in a semantic or latent level of meaning (Braun & Clarke, 2012).

**Phase 3: Searching for themes,** Once the data have been initially coded and collated, searching for themes can then take place where the analysis then starts taking shape (Noyes et al., 2008). According to Braun & Clarke (2012), a theme captures important details about the data with the research question and represent some form of a level of patterned response or meaning within the set of data. The development of the list of different codes across the data must be in place to sort and collate all the potential relevant coded data extracts into the themes(Noyes et al., 2008). Areas of similarity can be identified by reviewing coded data to identify overlap between codes (Braun & Clarke, 2012).

**Phase 4: Reviewing themes,** once the themes are devised, the reviewing of themes can then take place where refinement can be undertaken. The researcher determines if the theme in each coded data extract forms a coherent pattern (Noyes et al., 2008). New codes can be developed if there are inadequacies in the initial coding (Noyes et al., 2008), the developed themes in this phase are reviewed with the coded data as well as the entire coded data through a recursive process (Braun & Clarke, 2012). Themes should be checked against the collated extracts to explore if the themes work with the data, should that not be the case there might be a need to discard some codes or relocate some codes to another theme (Braun & Clarke, 2012).

**Phase 5: Defining and naming themes,** Aspects of each theme captured are determined and interesting points are identified. Each theme must be analysed in a detailed manner, themes should only be considered final once the data has been read thoroughly and the coding has been scrutinized at least twice. Researchers should be able to determine at the end of each phase what the themes are and what they are not (Noyes et al., 2008). The defined themes should enable the researcher to state what is unique and specific about each theme (Braun & Clarke, 2012).

**Phase 6: Reporting,** once themes are fully established, reporting can then take place together with the final analysis. The writing must be in a manner that provides a concise, coherent, logical and non-repetitive and interesting account of the data across and within the themes, researchers are encouraged to communicate the logic behind the process in which findings were developed in a manner that is accessible to a critical reader (Noyes et al., 2008). According to Braun, the purpose of reporting is to provide a compelling story of the data based on the analysis.

## 2.6 Conclusion

This chapter provided a layout and detailed description of the systematic literature review protocol, procedure, and methodology for conducting this systematic review. Outlining the process to be followed as well as steps and strategies to be carried out. From this formulated process and procedure, the study seeks to discover information from predetermined sources using the databases. What was key in the methodology was the development of the protocol. The protocol is a blueprint for conducting reliable and replicable research as required by the systematic literature review process. PICO and PRISMA methods were used for defining the research question and the procedure for selecting data. Electronic databases to be used for gathering information were listed. The inclusion and exclusion criteria were established to assist in selecting the final literature.

UNIVERSITY OF JOHANNESBURG

# Chapter 3 : Retrieval of documents

In this chapter, relevant articles will be retrieved following the systematic literature review methodology and the results will be documented in a form of a report. Results will be drawn out through the application of the systematic review protocol tabled out in Chapter 2. The PRISMA process will be followed to obtain results from the databases using the search keywords that will be grouped and tabled based on each database. Trend analysis to answer the research question through the selected primary studies will be used based on the total results obtained from the identified six databases.

## 3.1 Retrieval of documents per database

Relevant articles were retrieved from the electronic database through the application of the research protocol strategy. The research made use of the search key phrases in Table 2-1. The search keywords were applied consistently in databases except in one instance where “OR” was used instead of “AND”.

## 3.2 Step 1: Studies identification

This section will present details of data extraction per database, indicating keywords and methodologies used to retrieved relevant articles. Data extracted is summarised in Table 3-1. Details of data extracted per database is shown in Appendix A.

A total of 2013 documents were retrieved from the six databases. Table 3-1 illustrate a summary of documents retrieved per database.

**Table 3-1:Summary of the total retrieved document titles.**

| | | Data source | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Journal Article | Conference paper | Book section | Article in Press | Magazine | Thesis | **Total** |
| **Database** | ProQuest | 659 | 1 | | | 2 | | 662 |
| | IEEE | 43 | 141 | 88 | | 37 | | 309 |
| | Emerald | 221 | | 9 | | | | 230 |
| | Engineering Village | 113 | 315 | 17 | 1 | | | 446 |
| | Wiley Online | 20 | | 86 | | | | 106 |
| | ScienceDirect | 249 | 4 | | 7 | | | 260 |
| | **Total** | **1305** | **461** | **200** | **8** | **39** | | **2013** |

## 3.3 Step 2: Screening for removing duplicates

Screening for duplicates was done by making use of DOI numbers to identify duplicate articles from different databases. The identified duplicates were removed with the help of Endnote and by verifying duplicates through screening the DOI numbers of each retrieved document. A total of 633 duplicates were found and 1380 distinctive document titles remain. Table 3-2 illustrate how the remaining documents are categorised.

UNIVERSITY OF JOHANNESBURG

**Table 3-2: Summary of remaining distinctive document titles after removing duplicates**

| | | Data source | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Journal Article | Conference paper | Book section | Article in Press | Magazine | Thesis | **Total** |
| **Database** | ProQuest | 492 | | | | 2 | | 494 |
| | IEEE | 67 | 82 | 57 | | | | 206 |
| | Emerald | 141 | | 7 | | | | 148 |
| | Engineering Village | 65 | 189 | 11 | 1 | | | 266 |
| | Wiley Online | 11 | | 63 | | | | 74 |
| | ScienceDirect | 187 | | | 5 | | | 192 |
| | **Total** | **963** | **271** | **138** | **6** | **2** | | **1380** |

## 3.4 Step 3: Screening articles for inclusion based on abstract

### 3.4.1 Screening using word codes.

The first procedure applied was screening the retrieved documents using word codes which was based on the abstract from the retrieved literature. Endnote was used for exporting literature into Microsoft excel with document titles, abstract, authors, DOI numbers, date, etc. The article abstracts were screened through coding that was undertaken by applying the 55 keywords codes to screen the abstract of the 1380 distinctive documents to identify relevant documents. Table 3-3 illustrate the summary of the 55 keywords codes used. The keywords below were extracted from the modified PICO model discussed in chapter 2 using synonyms and related terms.

**Table 3-3: Summary of the 55 keywords codes.**

| | | | | |
|---|---|---|---|---|
| Employees | Cybersecurity | Knowledge | SCADA | Requirement |
| Workforce | Cybercrime | Education | Cyber | Public |
| Government | Culture | Training | Security | Cyber-literate |
| Engineering | Awareness | Resilience | Cyber-security | Learning |
| Water-sector | Skills | Response | Cyber-physical | Guideline |
| Technical | Training | Defence | Cyber-Specific | Challenge |
| Capacity | Behaviour | Threat | ICS | Change |
| Municipality | Mitigation | Capabilities | Wastewater | Cyberspace |
| Operations | Mindset | Solution | Sewer | Protect |
| Utility | Risk | Competence | Vulnerable | Prevent |
| Critical Infrastructure | Attack | Cyber-attacks | Resilient | Problem |

Screening the remaining 1380 documents was done by extracting abstracts of each literature and identify the number of keywords appearing from the abstract to get rid of irrelevant documents. The rigorous process followed in identifying relevant documents is indicated below:

- Retrieved all documents from Endnote and transferred them to Microsoft excel with abstracts and DOI numbers.
- Each document was arranged and put in each cell to better manage the documents.
- Abstracts of each document were reviewed to identify the number of keywords appearances.

UNIVERSITY OF JOHANNESBURG

- Searching for 55 keywords was done through the use of the "find" function in excel and they were highlighted.
- "COUNTBYFONTCOLOR" function in excel is used to count the number of keywords appearances.
- Documents with more than 25 keywords appearances in their abstract were selected.
- Appendix B indicates the results of the studies and the resulting word codes number of matches.

From the rigorous process above, 1215 documents were removed, and a total of 165 documents were selected for further reading the abstract to screening if the articles are relevant. See Appendix B with the studies and resulting word codes. See the table below with the summary of documents with more than 25 keywords appearances in their abstract. Table 3-4 below presents the summary of the documents with more than 25 keywords appearances.

**Table 3-4: Summary of documents with more than 25 keywords appearances in their abstract**

| | | Data source | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Journal Article | Conference paper | Book section | Article in Press | Magazine | Thesis | **Total** |
| **Database** | ProQuest | 41 | | | | | | 41 |
| | IEEE | 4 | 22 | 2 | | | | 28 |
| | Emerald | 20 | | | | | | 20 |
| | Engineering Village | 10 | 48 | 1 | | | | 59 |
| | Wiley Online | 4 | | | | | | 4 |
| | ScienceDirect | 13 | | | | | | 13 |
| | **Total** | **92** | **70** | **3** | | | | **165** |

## 3.4.2 Screening by reading abstracts in the documents.

The retrieved 165 documents through keywords codes were further screened by reading the abstracts to get rid of irrelevant documents. From reading the abstracts on a total of 165 documents, 134 documents were found to be irrelevant, and they were removed. This meant 30 literature documents remained, they will be screened for full text in the next step. The articles were assigned identification codes for ease of reference. The summary of the remaining 30 literature documents is summarised in Table 3-5 below.

**Table 3-5: Studies resulting from reading abstracts**

| Study ID | Reference | Title |
|---|---|---|
| S1 | (Adams, M. and Makramalla, 2015) | Cybersecurity skills training: An attacker-centric gamified approach |
| S2 | (AlMindeel & Martins, 2021) | Information security awareness in a developing country context: insights from the government sector in Saudi Arabia |
| S3 | (Alshaikh, 2020b) | Developing cybersecurity culture to influence employee behaviour: A practice perspective |
| S4 | (Carlton et al., 2019) | Mitigating cyber-attacks through the measurement of non-IT professionals' cybersecurity skills |
| S5 | (Catota et al., 2019) | Cybersecurity education in a developing nation: the Ecuadorian environment. Journal of Cybersecurity |
| S6 | (Chileshe & Heerden, 2012) | SCADA Systems in South Africa and their Vulnerabilities |

UNIVERSITY OF JOHANNESBURG

| Study ID | Reference | Title |
|---|---|---|
| S7 | (Chowdhury & Gkioulos, 2021) | Cyber security training for critical infrastructure protection: A literature review |
| S8 | (Ani et al., 2016) | Human capability evaluation approach for cyber security in critical industrial infrastructure |
| S9 | (Domínguez et al., 2017) | Cybersecurity training in control systems using real equipment |
| S10 | (Erdogan et al., 2021) | Developing cyber-risk centric courses and training material for cyber ranges |
| S11 | (Ficco & Palmieri, 2019) | An open-source cybersecurity training platform for realistic edge-IoT scenarios |
| S12 | (Jin et al., 2018) | Game based cybersecurity training for high school students |
| S13 | (Karabacak et al., 2016) | Regulatory approaches for cyber security of critical infrastructures |
| S14 | (Karampidis et al., 2019) | Industrial Cybersecurity 4.0: Preparing the Operational Technicians for Industry 4.0 |
| S15 | (Limba, T., Plėta, T., Agafonov, K. and Damkus, 2019) | Cyber security management model for critical infrastructure |
| S16 | (Malatji et al., 2020) | Validation of a socio-technical management process for optimising cybersecurity practices |
| S17 | (Mambile & Mbogoro, 2020) | Cybercrime's awareness, cyber laws and its practice in public sector Tanzania |
| S18 | (Mishra et al., 2015) | On building cybersecurity expertise in critical infrastructure protection |
| S19 | (Mishra et al., 2016) | A modular approach to teaching critical infrastructure protection concepts to engineering, technology and computing students |
| S20 | (Nagarajan et al., 2012) | Exploring game design for cybersecurity training |
| S21 | (Paulsen et al., 2012) | Creating a cybersecurity workforce and aware public |
| S22 | (Dahlian Persadha et al., 2016) | How inter-organizational knowledge sharing drives national cyber security awareness |
| S23 | (Prins et al., 2020) | Cybersecurity Awareness in an Industrial Control Systems Company |
| S24 | (Rege, 2016) | Incorporating the human element in anticipatory and dynamic cyber defense |
| S25 | (Khan et al., 2020) | SartCyber Security Awareness Measurement Model |
| S26 | (Rege et al., 2020) | A social engineering awareness and training workshop for STEM students and practitioners |
| S27 | (Turkanović et al., 2019) | An Example of a Cybersecurity Education Model |
| S28 | (Varga et al., 2018) | Information requirements for national level cyber situational awareness |
| S29 | (Da Veiga, 2016) | A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument |
| S30 | (Zhang et al., 2021) | Cybersecurity awareness training programs: a cost–benefit analysis framework |

UNIVERSITY OF JOHANNESBURG

The final 30 literature documents after screening by reading the abstract are divided as follows.

- Journal Articles: 16
- Conference Papers: 14

## 3.5 Screening for eligibility

Screening articles for eligibility was done through full-text screening by the application of the inclusion criteria and the exclusion criteria derived in chapter 2. The retrieved full documents will be used towards answering the research question.

**Table 3-6: Included studies**

| Study ID | Reference | Reason for Inclusion |
|---|---|---|
| S1 | (Adams, M. and Makramalla, 2015) | The study focuses on cybersecurity skills training. This study will add value to research analysis |
| S2 | (AlMindeel & Martins, 2021) | The study will add value to the research analysis on employee information security awareness |
| S3 | (Alshaikh, 2020b) | The study focuses on developing a cybersecurity culture to influence employee behaviour; this will add value to the research analysis |
| S4 | (Carlton et al., 2019) | The study looks into mitigating cyber-attacks through measuring cybersecurity skills, the study will add value to the analysis |
| S7 | (Chowdhury & Gkioulos, 2021) | This study will add value to the research as it focuses on cybersecurity training for protecting critical infrastructure. |
| S8 | (Ani et al., 2016) | This study will add value to the research, it focuses on understanding the employee cyber security knowledge, and skills capabilities for developing a skilled workforce. |
| S10 | (Erdogan et al., 2021) | The study focuses on cybersecurity training using cyber ranges. It will add value to research analysis |
| S11 | (Ficco & Palmieri, 2019) | This study will add value to the research, it focuses on cybersecurity education and training programs |
| S12 | (Jin et al., 2018) | The study focuses on game-based cybersecurity training. It will add value to research analysis |
| S14 | (Karampidis et al., 2019) | The study focuses on personnel training for identifying cybersecurity threats, this study will add value to the research analysis |
| S15 | (Limba, T., Plėta, T., Agafonov, K. and Damkus, 2019) | The study is focused on providing theoretical aspects of the cyber security management model which can be used to ensure the security of critical infrastructure |
| S18 | (Mishra et al., 2015) | The study will add value to the research analysis as it focuses on training in critical infrastructure protection |
| S20 | (Nagarajan et al., 2012) | The study will add value to the research analysis due to its focus on cybersecurity awareness and cyber skills training. |
| S21 | (Paulsen et al., 2012) | The study focuses on creating a cybersecurity workforce and aware public. |
| S22 | (Dahlian Persadha et al., 2016) | The study will add value to the research analysis due it's to the focus on Cybersecurity awareness. |
| S23 | (Prins et al., 2020) | The study will add value to the research analysis as it focuses on cybersecurity awareness levels and knowledge. |

UNIVERSITY OF JOHANNESBURG

| Study ID | Reference | Reason for Inclusion |
|---|---|---|
| S24 | (Rege, 2016) | The study focuses on developing anticipatory cybersecurity measures, this will be valuable to the research analysis. |
| S25 | (Khan et al., 2020) | The study will add value to the research analysis due it's to the focus on cybersecurity awareness and training. |
| S26 | (Rege et al., 2020) | The study focuses on developing a social engineering awareness and training program, this will be valuable to the research analysis. |
| S27 | (Turkanović et al., 2019) | The focus of the study is on the cybersecurity education model from the Information Systems and Information Technology perspective. |
| S28 | (Varga et al., 2018) | The study will add value to the research analysis due to its focus on acquiring cyber situational awareness. |
| S29 | (Da Veiga, 2016) | The study focuses on the measure of a cybersecurity culture; this will be valuable to the research analysis. |
| S30 | (Zhang et al., 2021) | The focus of the study is on cybersecurity, awareness training programs. |

After downloading and reading the full text of the 30 articles, S5, S6, S9, S13, S16and S17were found to be irrelevant and/or not applicable for this research. Table 3-7below illustrates reasons for exclusions.

**Table 3-7: Excluded studies**

| Study ID | | Reason for Exclusion |
|---|---|---|
| S5 | (Catota et al., 2019) | The study focuses on cybersecurity in the financial sector and information technology students. The study will not add value to the research analysis. |
| S6 | (Chileshe & Heerden, 2012) | The study focuses on technical aspects and not the human aspects of cybersecurity. The study was excluded because it will not add value to the research analysis. |
| S9 | (Domínguez et al., 2017) | The study does not address the in-depth human aspects of cybersecurity. Focuses on industrial control systems. |
| S12 | (Jin et al., 2018) | Study aimed at cybersecurity training for high school students and not employees. The study was excluded because it will not add value to the research analysis. |
| S13 | (Karabacak et al., 2016) | The study focuses on regulation in cybersecurity and not the human aspects in cybersecurity. |
| S16 | (Malatji et al., 2020) | The study focused on management processes for protecting assets against cybersecurity. |
| S17 | (Mambile & Mbogoro, 2020) | Articles gives focus on awareness of cybercrimes act and cyber law. |
| S19 | (Mishra et al., 2016) | The study focuses on integrating critical infrastructure protection into the undergraduate technological curriculum. |

After excluding seven studies, remains 23 studies will be taken through to the next section where quality assessment using a critical appraisal of the 10-questions listed in Table 2-4 will be applied. Below is the summary of the type of remaining studies.

## 3.6 Quality appraisal

Articles were assessed under the critical appraisal questions listed in Table 3-8. The quality appraisal of the selected studies followed the process below.

- Reading the journal article/conference paper
- Application of the critical appraisal questions
- Rate articles based on response to the appraisal questions.

The ten critical appraisal questions used to determine the reliability of the studies as illustrated in Table 2-4 are.

- Q1: Is there a clear statement of the aims of this research?
- Q2: Is there an appropriate research methodology?
- Q3: Is there an appropriate research design in the article that addresses the aims of the research?
- Q4: Is there an appropriate data selection strategy in line with the aims of the research?
- Q5: Does the data collection address the research issue appropriately?
- Q6: Are there adequate considerations of the relationship between the researcher and participants?
- Q7: Is there considerations on ethical issues that have been put in place?
- Q8: Is there a sufficiently rigorous data analysis?
- Q9: Is there a clear statement of findings?
- Q10: How valuable is the research?

The quality rating method per document is indicated below. The rating includes a scoring of 0,1,2 against each of the 10 critical appraisal questions. The rating of 0,1 and 2 represent whether the study is non-compliant, partial-compliant, and fully compliant, respectively. The quality rating is illustrated below.

Non-compliant : 0
Partially compliant : 1
Fully compliant : 2

UNIVERSITY OF JOHANNESBURG

**Table 3-8: Quality assessment**

| Study ID | Q1 | Q2 | Q3 | Q4 | Q5 | Q6 | Q7 | Q8 | Q9 | Q10 | Score/ 20 | Percentage Score |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S1 | 2 | 2 | 1 | 1 | 2 | 2 | 1 | 2 | 1 | 2 | 16 | 80% |
| S2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 20 | 100% |
| S3 | 2 | 2 | 2 | 2 | 2 | 2 | 0 | 2 | 2 | 2 | 18 | 90% |
| S4 | 2 | 2 | 2 | 1 | 2 | 1 | 2 | 2 | 2 | 2 | 18 | 90% |
| S7 | 2 | 2 | 1 | 2 | 2 | 2 | 1 | 2 | 2 | 2 | 18 | 90% |
| S8 | 1 | 1 | 1 | 2 | 2 | 0 | 0 | 1 | 1 | 1 | 10 | 50% |
| S10 | 2 | 2 | 2 | 1 | 1 | 1 | 0 | 2 | 2 | 2 | 15 | 75% |
| S11 | 2 | 1 | 1 | 0 | 2 | 0 | 0 | 1 | 1 | 2 | 10 | 50% |
| S14 | 2 | 2 | 2 | 1 | 1 | 0 | 0 | 1 | 2 | 2 | 13 | 65% |
| S15 | 2 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 2 | 1 | 11 | 55% |
| S18 | 2 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 2 | 10 | 50% |

| Study ID | Q1 | Q2 | Q3 | Q4 | Q5 | Q6 | Q7 | Q8 | Q9 | Q10 | Score/ 20 | Percentage Score |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S20 | 2 | 1 | 2 | 1 | 2 | 2 | 0 | 1 | 1 | 1 | 13 | 65% |
| S21 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 5% |
| S22 | 2 | 1 | 1 | 1 | 2 | 0 | 0 | 1 | 2 | 2 | 12 | 60% |
| S23 | 2 | 2 | 2 | 2 | 2 | 1 | 0 | 2 | 2 | 2 | 17 | 85% |
| S24 | 2 | 2 | 2 | 2 | 2 | 1 | 0 | 2 | 1 | 2 | 16 | 80% |
| S25 | 2 | 2 | 2 | 1 | 2 | 1 | 0 | 1 | 2 | 2 | 15 | 75% |
| S26 | 2 | 2 | 2 | 1 | 2 | 0 | 0 | 2 | 2 | 2 | 15 | 75% |
| S27 | 2 | 2 | 1 | 1 | 2 | 0 | 0 | 1 | 2 | 2 | 13 | 65% |
| S28 | 2 | 2 | 2 | 2 | 2 | 1 | 0 | 2 | 2 | 2 | 17 | 85% |
| S29 | 2 | 2 | 2 | 2 | 2 | 1 | 0 | 2 | 2 | 2 | 17 | 85% |
| S30 | 2 | 2 | 2 | 1 | 2 | 0 | 0 | 1 | 2 | 2 | 14 | 70% |

The maximum score that can be scored by an article is 20 points. The 22 included studies scored an average of 70%, the minimum score was 5% whereas the maximum score was 100%. S21 was found to be non-compliant based on the quality appraisal assessment and will therefore be excluded. The rest of the articles indicates good overall reliability of the selected studies. The performed research process is summarised in the PRISMA process diagram as illustrated in Figure 3-1 below.

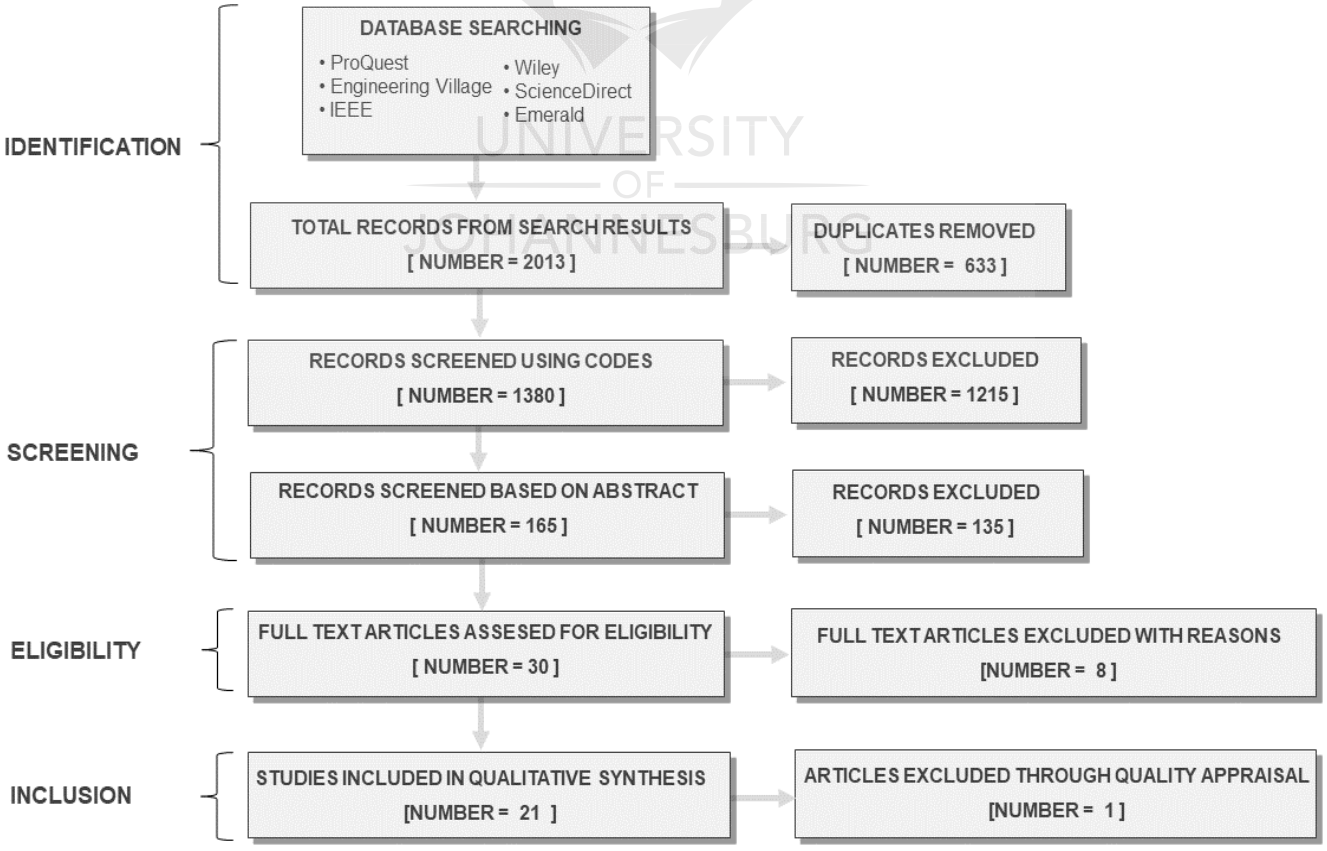


**Figure 3-1: PRISMA process flow diagram** (Liberati et al., 2009)

Six databases were used in the identification phase to search for literature using the search strategy. The search strategy returned 2013 literature documents, 633 of which were identified duplicates as a result of searching multiple databases. The remaining 1380 literature documents were subjected to screening. The first screening procedure involved the use of codes to identify literature that will help answer the research question. The codes screening process resulted in the retention of 165 pieces of literature, which then went through the second screening process, which involved reading abstracts. The second screening process resulted in the retention of 30 pieces of literature for full-text assessment, where eligibility was checked based on the inclusion and exclusion criteria that resulted in the exclusion of seven studies and inclusion of 23 studies. The 23 studies went through the quality appraisal and one study was found to be non-compliant based on the quality appraisal assessment and it was excluded. In the end, 21 studies from the literature were chosen for qualitative synthesis and analysis. The qualitative synthesis and analysis will be carried out in the next chapter.

## 3.7 Conclusion

In this chapter, all the retrieved articles were presented per database based on the study selection criteria steps defined in chapter 2. A total of 2013 studies were produced from the electronic database of which the majority of the studies were journaled articles and conference papers followed by book sections. The search strategy through the application of the Boolean search operation resulted in obtaining relevant and appropriate data. In terms of data acquisition, ProQuest produced the majority of the data extracted, followed by Engineering Village and IEEE. The use of Endnote and Microsoft excel made it possible to screen these many studies in an efficient and quality manner. From the systematic literature review process, 21 literature documents were selected for analysis. To maintain quality and reliability, the systematic literature review principles were followed to ensure objectivity in the data collection process and eliminate the risk of bias towards certain studies through quality appraisal. The extracted data will be analysed in the next section and results will be discussed.

UNIVERSITY OF JOHANNESBURG

# Chapter 4 : Analysis and Synthesis

In this chapter, the aim is to present the analysis and synthesis of the articles acquired from the primary studies where an electronic search was conducted independently in ProQuest, IEEE, Emerald, Engineering Village, Wiley Online and ScienceDirect. All these returned studies are listed in Table 3-6. The analysis and synthesis do not include the excluded articles in Table 3-7. 2013 studies were retrieved from the selected electronic databases from which the studies were taken through a rigorous screening process that made use of the PRISMA diagram methodology. A total of 30 studies were produced for full-text screening from which seven studies were excluded based on the exclusion criteria. The 21 remaining articles will be analysed in this chapter through the application of the thematic analysis technique.

Qualitative data analysis can be complex and diverse. There are different ways of analysing qualitative data, very often this depends on the type of data gathered. As previously indicated in Section 2.5.1, this research will follow the thematic analysis methodology to analysing the studies. As a qualitative method, thematic analysis can be used to analyse large qualitative data(Nowell et al., 2017). Thematic analysis is flexible in that it allows the researcher to determine themes and prevalence in several ways (Braun & Clarke, 2006a). The thematic analysis will follow six steps as illustrated in Table 2-5. The first step is familiarisation with the data, this step is necessary for the researcher to note initial ideas and transcribing the data from reading. The second step is generating initial codes where the author code interesting features in the data and collate relevant data before searching for themes, searching for themes is the third step where codes are then collated into potential themes. Themes are reviewed in the fourth stage by verifying if the theme works with the coded extract. Analysing and refining the specifics of each of them becomes the fifth stage before the last stage which is reporting on the analysis of selected extracts relating to the research question (Braun & Clarke, 2006b). The five stages that will be followed following Braun are indicated below:

1. Familiarisation with the data
2. Generating initial codes
3. Searching for themes
4. Reviewing the themes
5. Reporting

UNIVERSITY OF JOHANNESBURG

## 4.1 Familiarisation with the data

Researchers must immerse themselves with the data to familiarise themselves with the depth and breadth and depth of the data content (Nowell et al., 2017). Immersing with the data involves reading the data repeatedly in an active way while searching for meaning and patterns(Nowell et al., 2017). This initial stage deals with reading the data repeatably for familiarisation. In this stage patterns in the data are identified together with the common ideas within these studies. Subsequently, this will assist in generating codes and themes from the data set. This step is needed to enable the researcher to generate the initial category of ideas, also referred to as codes (Braun & Clarke, 2006a). The studies are grouped by the study identification numbers, the methodology followed by the type of study, the purpose of the study and the publication year. The aim of grouping these studies is to assist in a better understanding of the data by grouping the studies. Table 4-1 below indicates the list of the nine journal articles that were analysed from the selected 21 studies.

**Table 4-1: Analysis of journal articles**

| Study ID | Study Methodology | Type of Study | Purpose of the Study | Year |
|---|---|---|---|---|
| S1 | Literature Study | Journal Article | Building cybersecurity skills into a workforce. | 2015 |
| S2 | Case Study and Interviews | Journal Article | Understanding employee information security awareness. | 2019 |
| S3 | Case Study | Journal Article | Developing a cybersecurity culture. | 2020 |
| S4 | Case Study | Journal Article | Measuring the cybersecurity skills of non- IT professionals. | 2018 |
| S7 | Literature Study | Journal Article | Establishing Cybersecurity training for critical infrastructure. | 2021 |
| S11 | Literature Study | Journal Article | Using simulation to develop competitive cybersecurity training exercises and skills. | 2019 |
| S15 | Literature Study | Journal Article | Provide theoretical aspects of the cyber security management model. | 2017 |
| S25 | Literature Study | Journal Article | Cyber Security Awareness Measurement Model. | 2020 |
| S30 | Literature Study | Journal Article | Development of Cybersecurity awareness training Programs. | 2021 |

The remaining 12 from the total of 23 studies are conference papers as listed in Table 4-2 below. These conference papers were also grouped by the study methodology, study type and purpose of the study.

**Table 4-2: Analysis of conference papers**

| Study ID | Study Methodology | Type of Study | Purpose of the Study | Year |
|---|---|---|---|---|
| S8 | Literature Study | Conference Paper | Workforce Cyber Security Capability evaluation model | 2016 |
| S10 | Literature Study | Conference Paper | Using cyber ranges to train and develop cybersecurity skills and awareness | 2021 |
| S14 | Questionnaire | Conference Paper | Investigation of the security weaknesses | 2019 |
| S18 | Literature Study | Conference Paper | Integrating CIP into cybersecurity training | 2015 |
| S20 | Literature Study | Conference Paper | Teaching cybersecurity skills through gaming | 2012 |
| S22 | Interviews and Literature Study | Conference Paper | Relationship between inter-organizational knowledge sharing and creation of cyber security awareness behaviour. | 2016 |
| S23 | Case Study and Questionnaire | Conference Paper | determining the level of cybersecurity awareness in the organization | 2020 |
| S24 | Case Study | Conference Paper | Developing anticipatory cybersecurity measures. | 2016 |
| S26 | Case Study | Conference Paper | Design and development of social engineering awareness and training program | 2020 |
| S27 | Case Study | Conference Paper | Cybersecurity education model | 2019 |
| S28 | Questionnaire Survey | Conference Paper | Acquiring cyber situational awareness | 2018 |
| S29 | Literature Study | Conference Paper | Development of cybersecurity culture measuring instrument | 2016 |

UNIVERSITY OF JOHANNESBURG

## 4.2 Generating initial codes

Initial production of initial codes from the data takes place at this stage. Coding is used to allow the researcher to simplify and focus on specific characteristics of the data (Braun & Clarke, 2006a). At this stage, codes were developed through the process of forming categories based on elements shared within the data. The coding was developed with the consideration of the research question. A list of items that reoccurred in the studies data set were listed in Table 4-3 as initial codes. Throughout the stages, coding became a continuous and cyclical process that was done up to a point where the themes that were developed became satisfactory.

The studies were read with cognisance of the types of cybersecurity threats as the challenges and the reported methodology to mitigate these threats or challenges. The data was organised in the two categories of meaningful groups to represent material with common elements. Results are illustrated in **Table 4-3** below.

**Table 4-3: Initial codes**

| Study ID | Codes for challenges | Codes for mitigations |
|---|---|---|
| S1 | Employee carelessness and inability | Game-based training |
| S2 | Attackers luring employees | Information security awareness |
| S3 | Employee non-compliance | Cybersecurity culture |
| S4 | Employees poor cybersecurity skills | Cybersecurity skills |
| S7 | Human error | Cybersecurity training |
| S8 | Human error | Workforce cybersecurity capability |
| S10 | Data leakage | Cyber-risk centric learning |
| S11 | Lack of strong cybersecurity workforce | Open-source cybersecurity training |
| S14 | Identifying and responding to attacks | Cybersecurity awareness |
| S15 | Detecting and responding to attacks | Minimizing cybersecurity risks |
| S18 | Stolen or lost laptops | Flexible cybersecurity training |
| S20 | User lack of abilities | Game-based training |
| S22 | Human targeting | Cybersecurity awareness |
| S23 | Employee lack of threats awareness | Cybersecurity culture |
| S24 | Failure to discover incidents | Cybersecurity training |
| S25 | Targeting of end users | Cybersecurity awareness |
| S26 | Persuasion and manipulation | Cybersecurity awareness and training |
| S27 | Malicious insider | Cybersecurity education |
| S28 | Lack of threat intelligence | Cyber Situational Awareness |
| S29 | Human error | Cybersecurity culture |
| S30 | Human error | Cybersecurity awareness training |

UNIVERSITY OF JOHANNESBURG

## 4.3 Searching for themes

At this stage, themes for identifying the cybersecurity challenges and the corresponding themes for building cybersecurity knowledge emerged under the codes listed in Table 4-3. Codes with common features were allocated to the appropriate and relevant themes. The theme aims to capture important details in the data with the research question to present patterned response or meaning in the data set (Braun & Clarke, 2006a). Coding of text can be done in as many and different themes as they fit (Nowell et al., 2017). Table 4-4 below is a summary of themes generated for the cybersecurity challenges and mitigations.

**Table 4-4: Summary of generated themes**

| Study ID | Themes for cybersecurity challenges | Themes for mitigations |
|---|---|---|
| S1 | Security breach, Unauthorised access, negligence, malicious insider | Cybersecurity skills and training |
| S2 | Unauthorised access, negligence, social engineering, malware, ransomware/malware | Cybersecurity awareness and skills |
| S3 | Security breaches, social engineering | Cybersecurity culture |
| S4 | Security breaches, social engineering, malicious insider, ransomware/malware, stolen credentials | Cybersecurity skills |
| S7 | Unauthorised access, social engineering, malicious insider, ransomware/malware | Cybersecurity training |
| S8 | Security breaches, Unauthorised access, negligence, social engineering, Malicious insider, ransomware/malware, stolen credentials | Cybersecurity knowledge and skills |
| S10 | Security breaches, social engineering, ransomware/malware, stolen credentials | Cybersecurity skills and awareness |
| S11 | Security breaches, negligence, malicious insider, denial of service | Cybersecurity skills training |
| S14 | Security breaches, negligence, denial of service | Cybersecurity training |
| S15 | Security breaches, ransomware/malware, denial of service | Cybersecurity management |
| S18 | Security breaches, unauthorised access | Cybersecurity skills and training |
| S20 | Security breaches, unauthorised access, social engineering, ransomware/malware, stolen credentials | Game-based cybersecurity skills training |
| S22 | Security breaches, social engineering | Cybersecurity awareness |
| S23 | Security breaches, stolen credentials, denial of service | Cybersecurity awareness and skills |
| S24 | Security breaches, social engineering, malicious insider, ransomware/malware | Cybersecurity training |
| S25 | Security breaches, negligence, social engineering, ransomware/malware, stolen credentials | Cybersecurity awareness and training |
| S26 | Social engineering, malicious insider, ransomware/malware | Cybersecurity awareness and training |
| S27 | Malicious insider | Cybersecurity knowledge and skills |
| S28 | Security breaches | Cybersecurity awareness |
| S29 | Security breaches, negligence, social engineering, denial of service | Cybersecurity culture |
| S30 | Security breaches, social engineering, ransomware/malware, stolen credentials | Cybersecurity awareness training |

UNIVERSITY OF JOHANNESBURG

### 4.3.1 Themes for cybersecurity challenges

Eight themes were identified with identifying the cybersecurity challenges. These themes will assist 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 Table 4-3:

- Security breach
- Unauthorised access
- Negligence
- Social engineering
- Malicious insider
- Malware/Ransomware
- Stolen credentials
- Denial of service

The subsections below discuss the second recoding cycle that focuses on the salient features of the qualitative data in order to generate themes. The supporting secondary codes shown in Table 4-3 were used to organize groups with similar codes relating to the eight themes listed above.

#### 4.3.1.1 Security breaches

Codes tabulated in Table 4-5 were used for categorising the theme for security breaches.

**Table 4-5: Supporting codes for security breaches**

| Study ID | Secondary codes for challenges |
|---|---|
| S1 | Employee carelessness and inability |
| S3 | Employee non-compliance |
| S4 | Employees poor cybersecurity skills |
| S7 | Human error |
| S8 | Human error |
| S10 | Data leakage |
| S11 | Lack of strong cybersecurity workforce |
| S14 | Identifying and responding to attacks |
| S15 | Detecting and responding to attacks |
| S18 | Stolen or lost laptops |
| S20 | User lack of abilities |
| S22 | Human targeting |
| S23 | Employee lack of threats awareness |
| S24 | Failure to discover incidents |
| S25 | Targeting of end users |
| S28 | Lack of threat intelligence |
| S29 | Human error |
| S30 | Human error |

UNIVERSITY OF JOHANNESBURG

Sentences from the literature were extracted and paraphrased to give legitimacy to these codes, as briefly illustrated in the paragraph below.

According to Adams and Makramalla (2015), “over 70% of critical infrastructure providers in 13 countries had a data breach in 2013 and it was discovered that 54% of those breaches were caused by employee carelessness and abilities in preventing or reacting to data breaches” (S1), furthermore, Alshaikh indicated that “recent security assessments shows that employee noncompliance with organizational information security standards is the root cause of a considerable share of cybersecurity breaches” (S3). Chowdhury and Gkioulos (2021) mentioned that stolen data was shown to be the primary cause of 80% of data breaches (S7) whereas the security breach report from PWC’s indicated that “36% of vilest security breaches in 2013 were caused by human error” (S8).

Employee-caused vulnerabilities and breaches to organizational information systems continue to result in significant financial and information losses, vulnerabilities include poor cybersecurity skills(Carlton et al., 2019) (S4). There is therefore a need to develop courses to deal with data leakage through activities of cyber-risk awareness centric learning path (Erdogan et al., 2021) (S10). In the huge number of combinations of the ever present network and cyber-physical systems designs combined under the name Internet of Things, there is a risk of system violations and sensitive data leakage as the volume and strength of cyber-attacks grows due to a lack of an effective defence that involve a strong cybersecurity workforce (Erdogan et al., 2021) (S11).

Following the recent high-profile cybersecurity events involving Sony Pictures, Target, and Anthem, as well as the enormous OPM government data breach, cybersecurity has become a primary priority for the US government. The cybersecurity landscape includes cyberattacks, hacks, and high-profile data breaches. As a result, cybersecurity has become a top issue for both businesses and government institutions (S29).

Similarly a huge number of network intrusions and malicious assaults have occurred over the last several years, some of which include the enormous data breaches of customer information at Sony and Sony PSN (Paulsen et al., 2012) (S21). Security breaches not only result in significant financial losses, but also severely damage the trust of consumers, business partners, and stakeholders. Employees should be able to identify and respond to cyberattacks (Karampidis et al., 2019) (S14). According to PWC's security breach report, human mistakes were responsible for 36% of the worst security breaches in 2013 (Ani et al., 2016) (S8). Theft of resources occurs when unauthorized entities consume system resources, this is one of the most common types of critical infrastructure or industrial control system assaults, organisations should therefore be able to detect and respond to cybersecurity breaches (Limba, T., Plėta, T., Agafonov, K. and Damkus, 2019) (S15).

From stolen or lost laptops to large cyber-attacks, there are many news stories concerning security breaches in the business and governmental sectors (Mishra et al., 2015) (S18). Irrespective of the employee’s awareness, security breaches continue to affect many sectors (Dahlian Persadha et al., 2016)( S22). According to the Security Breaches Survey, the human component is becoming more of a worry, with three-quarters of big companies and a third of small companies reporting an employee-related breach (S29). Human errors are continuing to facilitate security breaches (S30). Schneider stated that” Only amateurs attack machines; professionals target people” (S22). The year 2014 was dubbed the "year of massive breaches," with many firms discovering problems two or

UNIVERSITY OF JOHANNESBURG

more years later. Organizations were unable to identify when the breach occurred, which meant estimating the scope of the event became difficult (Rege, 2016) (S24).

Data breaches are meant to be prevented through practising cybersecurity (Prins et al., 2020) (S23). In the future, cyber breaches will become more common, and the user will be the weakest trigger point. We need a continual cyber security awareness framework to address the issue of assaults caused by human error (Khan et al., 2020) (S25). Multiple systems vital to social operations were penetrated as a result of the attacks, according to a scenario-based analysis "If no attention is given to potential resourceful and intelligent adversaries who act purposefully in pursuit of their strategic goals, organizations may fail to detect and identify serious threats" (Varga et al., 2018) (S28).

#### 4.3.1.2 Unauthorised access

Table 4-6 below shows the list of codes that were used for categorising the theme for security breaches.

**Table 4-6: Supporting codes for unauthorised access**

| Study ID | Secondary codes for challenges |
|---|---|
| S1 | Attackers gaining access |
| S2 | Attackers luring employees |
| S4 | Unauthorised leakage of information |
| S8 | Manipulating insiders |
| S18 | Lack of necessary skills |
| S20 | Password weakness |

UNIVERSITY OF JOHANNESBURG

Key paragraphs relating to unauthorised access were extracted and paraphrased as illustrated below.

According to AlMindeel and Martins (2021) "one of the fundamental operational requirements of any type of organization, particularly government organizations, is information security. This entails protecting key information assets from security threats such as unauthorized access that can jeopardize their availability, integrity, and confidentiality. Attacker may succeed in obtaining sensitive information from employees by luring them to reveal secret personal information" (S2). Organisations can make use of cybersecurity to prevent damage that can be caused by the unauthorised use of electronic information and communication systems (Carlton et al., 2019) (S4). "Many industrial cyber-attacks have successfully defeated technological security solutions through Preying on human weaknesses in knowledge and skills, and manipulating insiders within organizations into unsuspectingly delivering entry and access to sensitive industrial assets" (S8). Adams and Makramalla (2015) stated that "one of the human vulnerabilities include third parties who have access to an organization's network" (S1).

Ani (2016) ascertain that cyber-attacks have been successful in defeating technical security systems by preying on human vulnerabilities in knowledge and skills, and persuading insiders within companies into supplying entry and access to critical industrial assets without their awareness, due to the majority of employees not being informed of security concerns, their activities may raise the risk of network breaches (S8). Computers, their

hardware and software, networks, and data should be secured from cyber thieves, hackers, and terrorists gaining unauthorized access to the Internet (Ani et al., 2016) (S8). Data is vulnerable to a range of risks, including unauthorized access, so it's critical to keep it safe (Mishra et al., 2015) (S18). Passwords safeguard your computers, online accounts and data, therefore it's critical to spread the word about the need of using strong passwords as the first line of protection (Nagarajan et al., 2012) (S20).

#### 4.3.1.3 Negligence

Secondary codes generating similarity in relation to employee negligence are shown in Table 4-7.

**Table 4-7: Supporting codes for negligence**

| Study ID | Secondary codes for challenges |
|---|---|
| S1 | Employee negligence |
| S2 | Employee behaviour |
| S8 | Misuse of technology |
| S14 | Employee negligence |
| S25 | Human negligence |
| S29 | Human carelessness and mistake |

Sentences that support this theme were extracted and paraphrased from literature to give legitimacy to the codes, as seen in the paragraph below.

Individual actors, according to AlMindeel and Martins (2021), may imperil an organization's security standing through negligence (S2). Of the “70% data breaches experienced in 13 countries; it was discovered that 54% of those breaches were caused by employee negligence” (Adams, M. and Makramalla, 2015) (S1). Adams and Makramalla (2015) mentioned a typical example to be “when an organizational insider clicks on a malicious link embedded in an email, oblivious to the potential harm that such a mistake can cause” (S1). Human negligence results in 90% of cyber-attacks (S25). It is also found that, human mistake and carelessness have been shown to account for at least 30% of the loss of private information in the context of cybersecurity (S29)

One of the human vulnerabilities includes employee negligence (Adams, M. and Makramalla, 2015) (S1). Bad practices raise a variety of concerns that are now hard to prevent with passive defensive measures alone. According to PWC research, 20% of terrible security breaches were caused by intentional misuses of technology, showing a user character characteristic (Ani et al., 2016) (S8). Employee carelessness, for example, accounts for 80% of the vulnerabilities exploited by attackers (Adams, M. and Makramalla, 2015) (S1). An example is when a former Tehama Colusa Canal Authority employee installed unauthorized software on a computer used to transfer water from the Sacramento River for agricultural reasons, resulting in service disruption. This is a good example of how an administrator's negligence may create harm to a business (Karampidis et al., 2019) (S14). There is a need for a continual cyber security awareness framework to address the issue of assaults caused by human error (S25).

### 4.3.1.4 Social engineering

The supporting codes relating to the theme “social engineering” are listed in Table 4-8. These secondary codes were used for support this theme.

**Table 4-8: Supporting codes for social engineering**

| Study ID | Secondary codes for challenges |
|---|---|
| S2 | Human behaviour-related attack |
| S3 | Identifying scam |
| S4 | Limited cybersecurity skills |
| S7 | e-mail phishing |
| S8 | Phishing |
| S10 | Structured query language injection attack |
| S20 | Attack on human judgment |
| S22 | Human targeting |
| S24 | Advanced persistent threat |
| S25 | Phishing |
| S26 | Persuasion and manipulation |
| S29 | Organization impersonation |
| S30 | Phishing scams |

The codes were given authenticity by paraphrasing sentences from the literature as indicated below.

“Social engineering which includes phishing attacks, drive-by-downloads, etc. is currently widely regarded as the most serious security threat to individuals and organizations” (Carlton et al., 2019) (S4). When used maliciously against organizations, “social engineering poses a significant threat to employees, influencing them into doing activities that could expose their company to serious security threats” (AlMindeel & Martins, 2021) (S2). Stolen data, which is frequently obtained through social engineering tactics like e-mail phishing, can be blamed for data breaches (S7).

An example of social engineering is when an attacker successfully obtains sensitive information from employees by luring them to reveal secret personal information such as their user account/password to steal their network identity and gain unauthorised access to their organization's systems, the consequences are dramatic (AlMindeel & Martins, 2021) (S2). Phishing attacks are a popular type of social engineering in which hackers produce phoney emails contaminated with harmful links and/or attachments and send them to an employee or group of workers (AlMindeel & Martins, 2021) (S2).The primary cause of data breaches is stolen credentials obtained through phishing (Ani et al., 2016) (S8).

Security regulations alone can no longer defend vital infrastructures due to the rapid evolution of social engineering. Even with strict security measures in place, hackers use social engineering phishing techniques to trick employees into revealing personal, social security, and other sensitive information (Nagarajan et al., 2012) (S20). Using social engineering strategies, for example, is thought to be one of the most crucial components of the attack approach (Rege, 2016) (S24). Human error/negligence is a common cause of cyber-attacks, which

leads to attacks like phishing and social engineering (Khan et al., 2020) (S25). Human skills and persuasion tactics are used in social engineering to gain unauthorised information, thus teaching people about it through good awareness and training programs is critical (S26).

There is a need to develop courses to deal with the awareness of phishing through activities of cyber-risk awareness centric learning path (Erdogan et al., 2021) (S10). New social engineering attacks such as phishing emails and viruses must be communicated to employees to create awareness (Alshaikh, 2020b) (S3). Given the growth, frequency, and sophistication of cybersecurity assaults, particularly those that utilize social engineering tactics like phishing, establishing a strong cybersecurity defence remains a challenge (S30).

#### 4.3.1.5 Malicious insider

The supporting secondary codes tabulated in Table 4-9 below are for the theme “malicious insider”.

**Table 4-9: Supporting codes for malicious insider**

| Study ID | Secondary codes for challenges |
|---|---|
| S1 | Insider threat |
| S4 | Human error or misuse |
| S7 | Malicious links and attachments |
| S8 | Malicious cyber events |
| S11 | Malicious activities |
| S24 | Persistent malicious actors |

UNIVERSITY OF JOHANNESBURG

Key paragraphs from the literature were taken and paraphrased to give legitimacy to these codes, as seen in the paragraph below.

According to Adamsand Makramalla (2015), one of the human vulnerabilities includes malicious insiders (S1). Carlton (2019) stated that “not all insider threats are malicious, 84% of reported insider data breaches were caused by an accidental act or failure to protect a computer, networking device, or disk” (S4). Ficco and Palmieri (2019) argue that malicious insiders offer a variety of difficulties that are now hard to avoid with solely passive protection methods (S11).

It has been proven that having additional cyber security experts can help with the accurate detection of dangerous cyber events and reduce the mistaken classification of non-threatening cyber events as malicious. Skills can assist users in making the best judgments and taking the appropriate actions to reduce or eliminate the occurrence of malicious occurrences (Ani et al., 2016) (S8). There is a need to develop courses to deal with insider threats through activities of cyber-risk awareness centric learning path (Erdogan et al., 2021) (S10). Malicious insiders offer a variety of difficulties that are now hard to avoid with solely passive protection methods (Ficco & Palmieri, 2019) (S11).

When an organizational insider clicks on a malicious link embedded in an email, oblivious to the potential harm that such a mistake can cause (Adams, M. and Makramalla, 2015)( S1). In West Point Carronade, pupils were sent malicious and non-malicious emails as part of an experiment. Students who have received practical instruction were more likely to detect and report fraudulent emails (Chowdhury & Gkioulos, 2021) (S7).

#### 4.3.1.6 Malware/ransomware

Table 4-10 below shows the list of secondary codes that were used for categorising the theme for malware/ransomware. Key brief paragraphs relating to unauthorised access were extracted and paraphrased as illustrated below.

**Table 4-10: Supporting codes for ransomware/malware**

| Study ID | Secondary codes for challenges |
|---|---|
| S2 | Ransomware breaches |
| S4 | Non-secure websites |
| S7 | Sabotage operations |
| S8 | System exploitation and sabotage |
| S10 | Technical vulnerabilities |
| S15 | Hijacking systems |
| S20 | Viruses, worms and trojan infections |
| S24 | Critical infrastructure targeting |
| S25 | Malware software |
| S30 | Malware infections |

UNIVERSITY OF JOHANNESBURG

According to a study conducted by Ferris Research, malware caused $130 billion in yearly economic damages worldwide in 2009 (Nagarajan et al., 2012) (S20). Over the last few years, adversaries have figured out how to create malware that is especially meant to attack the victim, and they've been pretty successful. This also demonstrates that enemies are far ahead of the game in terms of strategy and are technically capable of outpacing traditional controls (Khan et al., 2020) (S25). Critical infrastructure is increasingly being targeted by persistent cybercriminals that makes use of targeted (spear) phishing, malware, vulnerability exploits (S24).

According to technical studies reported by Chowdhury and Gkioulos (2021), “attackers used several tactics to obtain access to many computer systems, including attaching malware to third-party programs, e-mails, and websites. By doing so, the attackers are able to mount sabotage on operations” (S7). Furthermore, most employees are frequently oblivious of security dangers; as a result, their actions may raise the chance of virus, worm, and trojan infestations(Ani et al., 2016) (S8). There is a need to develop courses to deal with attacks such as ransomware through activities of cyber-risk centric learning path (Erdogan et al., 2021) (S10). One of the most common types of attacks on critical infrastructure or industrial control systems is information corruption, which occurs when data on a system or communications channel is a corruption of information (Limba, T., Plėta, T., Agafonov, K. and Damkus, 2019)(S15).

“Over the past few years adversaries have found ways to develop malwares which are specifically designed to hit the target and have also been quite successful as well” (S25). Social engineering assaults can also result in ransomware breaches. Self-propagating malware encrypts a victim's data and holds it hostage until a ransom is paid (AlMindeel & Martins, 2021) (S2). Given the growth, frequency, and sophistication of cybersecurity assaults, particularly those that involve malware, creating a strong cybersecurity defence remains a challenge (Zhang et al., 2021).

#### 4.3.1.7 Stolen credentials

Table 4-11 below is a list of secondary codes relating to the theme “stolen credentials”. Sentences that support this theme were extracted and paraphrased from literature to give legitimacy to the codes, as seen in the paragraph below.

**Table 4-11: Supporting codes for stolen credentials**

| Study ID | Secondary codes for challenges |
|---|---|
| S4 | Password exploitations |
| S8 | Weak password configuration |
| S10 | Password weakness |
| S20 | Password cracking |
| S23 | Poor access control |
| S25 | Password exposure |

“Stolen credentials was identified as one of the top three cyber threats by Verizon Enterprise Solutions (2016)” (Carlton et al., 2019) (S4). A PWC research reported that “stolen credentials obtained through phishing are the underlying cause of data breaches 80 percent of the time” (Ani et al., 2016) (S8). Despite the importance of social engineering, the top three cyber risks were classified as malware, the use of stolen credentials, and phishing. The inappropriate or abusive use of IT systems poses serious security threats to the whole industrial system. Security concerns may arise as a result of the use of weak passwords. Security risks that may arise as a result of weak password configuration, inappropriate use of personal mobile devices, unprotected web access, and inappropriate recognition and response to social engineering attacks (Ani et al., 2016) (S8).

One of the top data breaches in 2018 and 2019 include the LinkedIn and Facebook emails addresses as well as passwords that were exposed (Khan et al., 2020) (S25). Using tactics such as brute force assaults, dictionary-based attacks, and phishing, hackers are getting more proficient at breaking passwords. As a result, it's critical to raise awareness about the need of using strong passwords as the first line of security. Techniques for establishing, using, and changing strong passwords regularly can be given (Nagarajan et al., 2012) (S20).

UNIVERSITY OF JOHANNESBURG

#### 4.3.1.8 Denial of service

The secondary codes tabulated in Table 4-12 were used for categorising the theme for security breaches.

**Table 4-12: Supporting codes for denial of service**

| Study ID | Secondary codes for challenges |
|---|---|
| S11 | Protecting critical assets |
| S14 | Industrial operational security |
| S15 | Denying access to authorised users |
| S23 | Software and control system vulnerability |
| S29 | Network penetration |

Sentences from the literature were extracted and paraphrased to give legitimacy to these codes, as briefly illustrated in the paragraph below.

Denial of service attacks or distributed attacks raises a variety of difficulties that are now hard to avoid with solely passive security measures (Ficco & Palmieri, 2019) (S11). According to Karampidis (2019), "a former Tehama Colusa Canal Authority employee placed illegal software on a computer used to divert water from the Sacramento River for agricultural purposes in 2007. The supervisory control and data acquisition system was infected by this program (SCADA)". That incident resulted in the denial of service (Karampidis et al., 2019) (S14).

One of the most common types of attacks on critical infrastructure or industrial control systems is denial-of-service, which results in authorized users being denied access to the system (Limba, T., Plėta, T., Agafonov, K. and Damkus, 2019)(S15). Denial of service attacks against software on industrial control platforms was among the common vulnerabilities listed by the National Institute of Standards and Technology (NIST) in their Guide to Industrial Control Systems (ICS) Security (Prins et al., 2020) (S23). Denial of service is one of the cyber-attacks experienced by organisations "employees' adherence (or lack thereof) to security procedures is considered to be the greatest challenge to organizations" (Da Veiga, 2016) (S29).

### 4.3.2 Themes for methods of building cybersecurity knowledge

Four themes were identified with the mitigations indicated in Table 4-3. The first theme (cybersecurity skills/knowledge) assisted in identifying the cybersecurity knowledge required for employees. The second theme (cybersecurity awareness) and the third theme (cybersecurity culture) looked at finding meaning in what organisations can do to urge cybersecurity culture and awareness. Overall, the first, second and third themes assisted in answering the research question. The fourth and last theme focused on identifying the types of general employee cybersecurity training methods that can be undertaken to improve cyber resilience. The identified training methods will further be used to develop a model to train employees in cybersecurity. The themes below were developed based on the codes retrieved from Table 4-3:

- Cybersecurity skills and knowledge
- Cybersecurity awareness
- Cybersecurity culture

- Cybersecurity training

The subsections below discuss the themes together with the supporting codes and reports on the themes.

#### 4.3.2.1 Cybersecurity skills and knowledge

Similar codes relating to cybersecurity skills and knowledge were categorised as tabulated in Table 4-13 below.

**Table 4-13: Cybersecurity skills and knowledge supporting codes**

| Study ID | Codes for Mitigations |
|---|---|
| S1 | Cybersecurity skills and training |
| S2 | Cybersecurity awareness and skills |
| S4 | Cybersecurity skills |
| S8 | Cybersecurity knowledge and skills |
| S10 | Cybersecurity skills and awareness training |
| S18 | Cybersecurity skills and training |
| S23 | Cybersecurity awareness and skills |
| S27 | Cybersecurity knowledge and skills |

To give authenticity to these codes, sentences from the research were taken and paraphrased as seen in the paragraphs below.

UNIVERSITY OF JOHANNESBURG

"Organisational attitude towards cybersecurity lies in the workforce's knowledge and skills" (Ani et al., 2016) (Ani et al., 2016) (S8), for this reason, top business executives, governmental agencies, and university researchers have all recognized the importance of developing cybersecurity skills and increasing knowledge among the workforce and leadership (Adams, M. and Makramalla, 2015) (Adams, M. and Makramalla, 2015) (S1). Cybersecurity skills (e.g., preventing malware, PII theft, and work information system (WIS) breaches) refer to a person's technical understanding, expertise, and experience with the hardware and software required to implement IS security and mitigate cyber assaults (AlMindeel & Martins, 2021) (S2).

According to Carlton (2019) and Khan (2020), more than 90 per cent of cyber threats to organisations are due to user mistakes as a result of poor cybersecurity skills (Carlton et al., 2019)(S4). Successful attacks on the workforce are also due to inappropriate or improper behaviour due to a lack of knowledge and skills that can counteract malicious actions (Ani et al., 2016) (S8). Employees can be easily attacked if they do not have a solid level of information technology skills (AlMindeel & Martins, 2021) (S2), Adamsand Makramalla (2015) stated that knowing the type of attackers, their motivation, resources, and knowledge/skills are important to develop and implement solutions to reduce cybercrimes (Adams, M. and Makramalla, 2015) (S1).

Ani (2016) prescribed capability as a product of knowledge, skills as well as tools whereas Carlton (2019) interpreted skill as a merger of abilities, experience, and knowledge that makes users perform well (S4 & S8).

Carlton (2019) further stated that the protection or defence against cyberattacks involves the human ability and technical aspects of cybersecurity (Carlton et al., 2019) (S4). Adamsand Makramalla (2015) concluded that the leadership together with the employees that were responsible for taking the necessary steps to respond to the cyberattack on the data breach of Target Corporation in 2013, lacked the necessary knowledge and skills (Adams, M. and Makramalla, 2015) (S1). The authors propose the use of a gamification approach to improving employees' capability in preventing or reacting to data breaches. It is crucial to note that organisational cybersecurity capability to guide human's behaviour into reaching cybersecurity assurance depends on the efficiency and responsiveness of the workforce (Ani et al., 2016) (S8).

According to AlMindeel and Martins (2021), a solid level of information technology skills was deemed the first thing that employees need to have to grasp possible loopholes and risks, authors further stated that employees should have a fundamental knowledge base that comprises sophisticated skills in computer security that will enable them to recognise potential security threat, foresee impact and initiate suitable responses (AlMindeel & Martins, 2021) (S2).

Carlton (2019) stated that cybersecurity skills that include prevention of malware, and the theft of personally identifiable information, as well as breaches on work information systems, is linked to an individual's ability, technical knowledge and experience surrounding the software and hardware required to carry out information systems security to mitigate cyberattacks. Employees may work in an insecure manner due to lack of skills, or human error or poor security tool usability. An individual can achieve full competency over time by obtaining additional knowledge, experience, and ability (Carlton et al., 2019) (S4).

The workforce should have diagnostic abilities to anticipate, spot and react to cyber-specific incidents, the authors also state that the skills and knowledge of the workforce are where the attitude of an organisation towards cybersecurity lie. Also, skills and knowledge have the valued characteristics that act for the workforce cybersecurity capability (Ani et al., 2016) (S8). Technological security solutions have been successfully defeated by preying on human weakness in skills and knowledge (Ani et al., 2016) (S8). The current, as well as the future engineers/technicians that work together with or with industrial 4.0 control systems, must know the different types of attacks that can be made on operational technologies (OT) networks or critical infrastructure.

Knowledge of attackers and their characteristics was pointed out as important when producing and implementing solutions to lessen cyber-crimes (Adams, M. and Makramalla, 2015) (S1). Knowing the cyber attacker characteristics such as the type of attacker is important in developing accurate profiling for producing and implementing solutions. Expert knowledge is required to prepare for disasters and attacks (Mishra et al., 2015) (S18). Understanding the types of invaders and their interests was pointed out as the first important thing by Limba and Plėta (2019). Critical infrastructure systems can be secured by anticipating adversary's moves by understanding how to assume characteristics of adversaries by understanding the adversary's movements and decision making associated with these movements (Rege, 2016) (S24).

Eight attacker types were identified by Adamsand Makramalla (2015) to be (i) *Script kiddies* who rely on existing tools such as exploiting programs, (ii) *Cyber-punks* who write a virus and exploit programs, (iii) *Insiders* who are within the organisation and bring about intentional and unintentional harm (iv) *Petty thieves* are attackers that carry out online fraud such as hijackings for ransom, (v) *Grey hats* usually attack systems to find flaws and prove

their abilities (vi) Professional criminals are hired hackers to infiltrate systems (vii) Hacktivists are attackers who are driven by ideology this include terrorist group. (viii) *Nation states* that are presumed to be working for a governmental body, target the enemy's systems.

Eight knowledge areas were declared by the Joint Task Force that presents the core knowledge a cybersecurity expert should understand and covers, this includes, (i) Data Security, (ii) System Security, (iii)Software Security, (iv) Human Security, (v) Organizational Security, (vi)Societal Security, (vii) Component Security, and (viii)Connection Security (Turkanović et al., 2019) (S27). The connection between these knowledge areas can be understood through six crosscutting concepts that are: (i)Confidentiality, (ii) Integrity, (iii) Availability, (iv) Risk, (v)Adversarial Thinking, and (vii) Systems Thinking (Turkanović et al., 2019) (S27).

Cybersecurity vulnerabilities to industrial control systems originate from a point where there is great connectivity to the system and where access control becomes the weakest, four domains of cyber vulnerabilities with different attack vectors were indicated. These domains are (i) IT, (ii) ICS, (iii) communication and (iv) physical domains (Limba, T., Plėta, T., Agafonov, K. and Damkus, 2019) (S15). Through the exploitation of vulnerabilities, a cyberattack is said to frequently develop in five different stages. These stages are (i) vulnerabilities in software or system or organisation, (ii) Exploitation of the vulnerability for taking control in the system, (iii) payload through malware or malicious code, (iv) infection of the system after exploitation, and then (v) attack where the physical damage can happen. (Limba, T., Plėta, T., Agafonov, K. and Damkus, 2019) (S15).

Developers, users, and support personnel of industrial control systems must grasp the idea of how to implement cybersecurity and must have the knowledge and understanding of the associated threats, vulnerabilities as well as risks of the technology or system (Prins et al., 2020) (S23).

UNIVERSITY OF JOHANNESBURG

#### 4.3.2.2 Cybersecurity awareness

The supporting codes relating to the theme for cybersecurity awareness are listed in Table 4-14. These codes for mitigations were used for categorising this theme.

**Table 4-14: Cybersecurity awareness supporting themes and codes**

| Study ID | Codes for Mitigations |
|---|---|
| S2 | Cybersecurity awareness and skills |
| S10 | Cybersecurity skills and awareness |
| S22 | Cybersecurity awareness |
| S23 | Cybersecurity awareness and skills |
| S25 | Cybersecurity awareness and training |
| S26 | Cybersecurity awareness and training |
| S28 | Cybersecurity awareness |
| S30 | Cybersecurity awareness training |

The codes listed in the Table 4-14 were given authenticity by paraphrasing sentences from the literature as indicated below.

AlMindeel and Martins (2021) consider Information security awareness as a safeguard against an employee's lack of understanding about security hazards to which they may be exposed if effective detection and identification are not carried out in advance (AlMindeel & Martins, 2021) (S2). Information security awareness provides an opportunity for employees to have a better understanding of an organization's policies and rules (Dahlian Persadha et al., 2016) (S22).

AlMindeel and Martins (2021) consider Information security awareness as a safeguard against an employee's lack of understanding about security hazards to which they may be exposed if effective detection and identification are not carried out in advance. (AlMindeel & Martins, 2021) (S2). The potential lack of knowledge about potential cyber threats by employees who can fall victim to without properly identifying or detecting the security threat can be protected through Information security awareness which is seen as a safeguarding aspect (AlMindeel & Martins, 2021) (S2). Information security awareness provides an opportunity for employees to have a better understanding of an organization's policies and rules (Dahlian Persadha et al., 2016) (S22). Systematizing knowledge dissemination beyond regular communication efforts is required for information security awareness to have the intended impact and operate effectively. (Prins et al., 2020) (S23).

Enhancing employees' cybersecurity awareness becomes crucial at a workplace where cyber-threats are a regular occurrence (AlMindeel & Martins, 2021) (S2), as these threats of cyberattack keep rising, cybersecurity awareness becomes an essential factor (Dahlian Persadha et al., 2016) (S22). Human error due to the lack of cybersecurity knowledge and awareness was indicated as one of the leading causes of cyber-incidents (Prins et al., 2020) (S23). As a result, it's critical to remember that the ultimate purpose of cyber threats and cyberattacks are humans, to prevent victimization it is therefore important to increase awareness of humans in cybersecurity (Dahlian Persadha et al., 2016) (S22).

Employee awareness and readiness are improved by investing in cybersecurity awareness training; nevertheless, the design of cybersecurity awareness and training should drive employees to create compliant behaviours (Rege et al., 2020)(S26).Senior managers with various functions at the organizational level can contribute unique insights in the production and integration of information security awareness views., how conversations around the information are developed on teams, how risk is assessed, and defence improved as well as the making the overarching choice to improve information security (AlMindeel & Martins, 2021)(S2).

Formal and experiential security training is thought to be the cornerstone for information security awareness understanding (AlMindeel & Martins, 2021) (S2). There are three steps into developing a successful cybersecurity awareness and training program, this includes (i) program design, (ii) material development and (iii) implementing the program. Such a program can enhance the understanding of attack methods and common characteristics of the targets (Rege et al., 2020) (S26), overall cybersecurity awareness is the knowledge of the threats that may arise in a company's cyber domain (Dahlian Persadha et al., 2016) (S22).

Cybersecurity awareness is critical in an organisation, Prins (2020) suggest the following parallel approaches in improving awareness and skills of employees; (i) Awareness programs must be implemented to increase awareness on an ongoing basis, (ii) training frameworks must be established to focus on countermeasure training and lastly (iii) the effectiveness of the program must be evaluated continuously (Prins et al., 2020)(S23)

UNIVERSITY OF JOHANNESBURG

To increase cybersecurity awareness, one must consider the technical, operational, organisational, and external factors (Dahlian Persadha et al., 2016) (S22). Developing inter-organisational knowledge sharing is important to create or establish a national cybersecurity awareness (Dahlian Persadha et al., 2016) (S22). The ability to identify cyber risk is considered the most important, this includes (i) identifying and presenting the current situation, (ii) assessing the impact or threat posed by that situation and (iii) projecting as well as assessing the situation's impact or threat (Dahlian Persadha et al., 2016) (S22)

Adequate situational awareness is critical for mitigating the effects of cyberattacks; good performance is linked to good situational awareness and limited situational awareness can lead to errors and poor performance. Full cyber situational awareness for cyber defence can be achieved by meeting seven requirements: (i) awareness of the current situation (ii) awareness of how situations evolve, (iii)assessment of plausible futures of the current situation, (iv)awareness of the quality and trustworthiness of the situational awareness information, (v) awareness of why and how the current situation is caused, (vi)awareness of adversary behaviour, and (vii) awareness of the impact of the attack (Varga et al., 2018)(S28).

The first beneficial line of defence should be about creating awareness of the importance of creating strong passwords (Nagarajan et al., 2012) (S20). Knowledge sharing was also considered beneficial in developing critical awareness based on experiences of co-workers (AlMindeel & Martins, 2021) (S2) For information security awareness to become an accepted mechanism that does not negatively affect work operations, careful planning and integration with routine work activities were seen as critical. (AlMindeel & Martins, 2021) (S2). The greatest impact on awareness can be achieved by ensuring that awareness material is quickly accessed and mobilised (AlMindeel & Martins, 2021) (S2).

According to Chowdhury & Gkioulos (2021) the main challenges that are faced when developing an awareness program are; the selection of an appropriate programme and the most effective method, the application of an adaptive method for continuous evaluation and modification of the program and lastly the use of the most up-to-date technology combined with the most appropriate tools to convey the message

UNIVERSITY OF JOHANNESBURG

Risk-taking was determined to below, and information security knowledge was high in individuals who are open to experience, honest and aggregable (AlMindeel & Martins, 2021) (S2). To comprehend information security awareness initiatives and their consequences on security behaviour, it is necessary to know both internal and external elements that can influence awareness levels, AlMindeel and Martins (2021)(AlMindeel & Martins, 2021)(S2) found that information security awareness can be positioned as an important predictor of the employees' security behaviour with employees' desire to act in a secure manner that is consistent with the organization's information security policy.

Alshaikh (2020b)indicated that cybersecurity campaigns should be aligned with external and internal campaigns to reduce employees demand on time. Carlton (2019) argues that although cybersecurity awareness gives employees exposure, it is restricted and only a short-term strategy and organizations fail to emphasize the importance of skills in cybersecurity workforce preparation by relying just on awareness initiatives.

A proper method for measuring the effectiveness of an awareness program should be in place, where the wealth of awareness towards cybersecurity can be drawn by developing a success tracking equation to check the effectiveness of the solutions implemented (Khan et al., 2020) (S25).

#### 4.3.2.3 Cybersecurity culture

The supporting codes for the cybersecurity culture theme are shown in Table 4-15. To give authenticity to these codes, sentences from the research were taken and paraphrased as seen in the paragraph below.

**Table 4-15: Cybersecurity culture supporting codes**

| Study ID | Codes for Mitigations |
|---|---|
| S3 | Cybersecurity culture |
| S29 | Cybersecurity culture |

A national cybersecurity culture enhances the security and resilience of a country's critical infrastructure (Da Veiga, 2016)(S29) According to (Khan et al., 2020), it is worth noting that a culture of excellent security practices can be fostered through ongoing and dynamic training and awareness.

Good security behaviours can be instilled by fostering a cybersecurity culture to shift attitude perceptions(Alshaikh, 2020b)(S3), risks from humans in cyberspace can be minimised by promoting a security culture at an individual, organisational, national, and international level (Da Veiga, 2016)(S29), therefore organizations must take a comprehensive approach to develop a cybersecurity culture in which security is everyone's responsibility and doing the right thing is the standard (Alshaikh, 2020b)(S3). Safely, security and privacy can be promoted or inhibited through the emergence of cybersecurity culture when interacting in cyberspace (Da Veiga, 2016) (S29).

Alshaikh (2020b) stated that Regular communication, awareness, training, and education initiatives embed cybersecurity culture in the behaviour of humans in an organizational context to protect information processed by the organization through compliance with the information security policy and an understanding of how to implement requirements cautiously and attentively. When it comes to preventing security, breaches caused by employee non-compliance with company security standards, cybersecurity culture becomes critical (Alshaikh, 2020b)(S3). Activities in an organisation such as the behaviour of employees as individuals and the vision of the management are the basis from which organisational culture develops (Da Veiga, 2016) (S29).

Security culture that can influence change on employees' behaviours was studied through identifying five key initiatives, these initiatives include (i) identifying essential cybersecurity behaviours; (ii) establishing a cybersecurity champion network; (iii) producing a brand for the cybersecurity team; (iv) creating a cybersecurity hub; and (v) connecting security education, training, and awareness operations with internal and external campaigns (Alshaikh, 2020b) (S3).

A national cybersecurity culture enhances the security and resilience of a country's critical infrastructure (Da Veiga, 2016)(S29) It's also worth noting that a culture of excellent security practices can be fostered through ongoing and dynamic training and awareness (Khan et al., 2020). Measuring and quantifying the culture of

cybersecurity could aid the development of strategies and programs to assist in promoting safe cyberspace (Da Veiga, 2016) (S29).

#### 4.3.2.4 Cybersecurity training

Similar codes linked to cybersecurity training were categorised as tabulated in Table 4-16below. To authenticate these codes, sentences from the literature were taken and paraphrased as seen in the paragraph below.

**Table 4-16: Cybersecurity training supporting codes**

| Study ID | Codes for Mitigations |
|---|---|
| S1 | Cybersecurity skills and training |
| S7 | Cybersecurity training |
| S10 | Cybersecurity skills and awareness training |
| S11 | Cybersecurity skills training |
| S14 | Cybersecurity training |
| S15 | Cybersecurity management |
| S18 | Cybersecurity skills and training |
| S20 | Game-based cybersecurity skills training |
| S24 | Cybersecurity training |
| S25 | Cybersecurity awareness and training |
| S26 | Cybersecurity awareness and training |
| S30 | Cybersecurity awareness training |

UNIVERSITY OF JOHANNESBURG

"Employees cannot be expected to avoid, report, or remove security threats without going through proper cybersecurity training. Organisations limit security training to the security team members and normal users are not given priority when it comes to cybersecurity training for employees"(Khan et al., 2020) (Khan et al., 2020)(S25). Additionally, for employees to recognise threats and take appropriate action to reduce the cyber risk they must receive proper cybersecurity training (Zhang et al., 2021)(Zhang et al., 2021)(S30).

Employees cannot be expected to avoid, report, or remove security threats without going through training. Organisations limit security training to the security team members, normal users are not given priority when it comes to cybersecurity training for employees (Khan et al., 2020) (S25). For employees to recognise threats and take appropriate action to reduce the cyber risk they must receive proper training (Zhang et al., 2021) (S30). Cyberattacks cannot be prevented or mitigated by implementing the latest technologies, there must be provision for ongoing personnel training. Stronger cybersecurity training is the best cybersecurity investment (Zhang et al., 2021) (S30).

Cybersecurity threats can be understood by knowing actions that must be taken to reduce ongoing attacks, this can be achieved through developing an ability to learn how to manage incidents and reduce the effects of successful attacks (Limba, T., Plėta, T., Agafonov, K. and Damkus, 2019)(S15).Rege (2016) identified five key areas for understanding anticipatory cyberdefense in intrusion chains that include (i) understanding adversarial

adaptability (ii) understanding the significance and characteristics of the various stages, (iii) adversarial decision-making, (iv) adversarial group dynamics, and (v) intrusion chain consistency and validation (Rege, 2016)(S24).

There is a need for trained employees to be capable of spotting potential cyber-threats and being prepared to respond in an adequate manner when the attack is identified (Karampidis et al., 2019) (S14) User awareness and training was reported as a key factor in the success of cyberattacks even though a best method and measures for cybersecurity training is yet to be reached (Chowdhury & Gkioulos, 2021) (S7). The ability to detect malicious emails can be achieved through practical training (Chowdhury & Gkioulos, 2021). (Chowdhury & Gkioulos, 2021) (S7). There has been a lack of critical infrastructure protection training programs for employees who are responsible for maintaining operations of critical assets (Mishra et al., 2015) (S18).

Employees can be able to plant malware after being trained through the use of the gamification approach where the employee develops desirable skills such as (1) prevention, (2) anticipation, (3) reaction, and (4) response (Adams, M. and Makramalla, 2015) (S1). Employees can also use cyber ranges to learn new techniques, improve, and test their abilities, as well as respond to threats and solve real-world cybersecurity issues. (Ficco & Palmieri, 2019) (S11) Cyber-ranges can be used to develop solutions that can prevent, detect, mitigate, recover, and evaluate the impact of an assault (Ficco & Palmieri, 2019) (S11).

According to Adamsand Makramalla (2015), it is through the gamified cybersecurity skills training approach, organisations can promote the prevention, anticipation, reaction and response sequence. It is difficult to hold employees' attention on training content without immersive and interactive game-elements, hence more hands-on immersive and interactive skills training for all employees is essential (Adams, M. and Makramalla, 2015)(S1), Another form of training that focuses mainly on hands-on exercises is cyber ranges, this form of training focuses on specific cybersecurity roles and skills that are ready to be integrated as part of a security training (Erdogan et al., 2021)(S10). Mishra (2015) presented a modular training strategy in which assessments involve hands-on experience in planning, implementing, and verifying the solutions (Mishra et al., 2015) (S18). Administrators can be trained by assuming the position of a hacker and attempting to penetrate a system using various tactics (Nagarajan et al., 2012) (S20).

UNIVERSITY OF JOHANNESBURG

Chowdhury and Gkioulos (2021) indicated that conventional or alternative methods of cybersecurity training were chosen over traditional or alternative methods that provided hands-on experience in the form of training scenarios and team-based activities. (Chowdhury & Gkioulos, 2021)(S7). Nagarajan (2012) further states that the disadvantage of most training programs is that they do not push students to think on their feet and apply what they have learned. There is therefore a requirement for prior hands-on experience in handling security events that takes place in a stressful environment (Nagarajan et al., 2012) (S20). In a program designed and presented by Rege (2020) participants used information provided on cybersecurity awareness and training to apply it in a hands-on training activity.

Khan (2020)suggest the model called the Analyse-Predict-Aware-Test (APAT) approach for (i) analysing the trends, (ii) predicting the behaviour, (iii) awareness based on user profile and, (iv) testing the effectiveness whereas Nagarajan (2012)suggest the use of gaming in teaching users the requisite cybersecurity skills because skills of users are wide-ranging, using games is capable of training a wide range of users in an engaging format (Nagarajan et al., 2012) (S20).

Erdogan (2021) developed a method for developing cyber-risk centric courses and training material. The method has 4 stages with the first stage being the identification of target user roles and the skills to be trained, once those roles and skills have been identified then the second step follows which involves associating the roles and skills to a standard cyber-risk assessment process before doing step three where the course is described considering the roles, skills, and risk-assessment process. (Erdogan et al., 2021) (S10)

Rege (2016)argues that profiling advanced president threats are crucial for developing anticipatory defence measures by understanding how adversaries adapt in various incursion chains, defenders can engage the adversary immediately if they invest in training staff to proactively identify data traffic., this improves real-time detection (Rege, 2016)(S24). Ficco and Palmieri (2019)push for more advanced cybersecurity education and training programs to be made available because today's cyberinfrastructure is complex, it necessitates the acquisition of specialized security-oriented skills by many actors to protect vital systems and data from cyberthreats and attacks. (Ficco & Palmieri, 2019) (S11).

The National Initiatives for Cybersecurity Education (NICE) and the Cybersecurity Workforce Framework (NICE Framework) has played a key role in the development of numerous cybersecurity awareness and training programs, tools, and modules (Paulsen et al., 2012) (S21). The comprehensiveness of the information outlined in the NICE documentation has been criticised by many researchers due to the inability of the framework to effectively cover multiple groups of interdisciplinary workforces (Chowdhury & Gkioulos, 2021) (S7). It is crucial to note that the NIST NICE Cybersecurity Workforce Framework emphasized skills training that is geared at employment in technical security rather than fundamental cybersecurity knowledge (Nagarajan et al., 2012) (S20).

Mishra (2015)proposed a flexible training framework that incorporates the NIST guidelines as well as the NICE initiative's suggestions. This course also includes critical infrastructure protection as part of the cybersecurity curriculum. The training framework is offered through a set of self-contained instructional modules that can be used independently or as part of a larger course. The modules address security's physical, human, and cyber aspects. (Mishra et al., 2015)(S18). Rege (2020) stated that the use of the NIST framework offered an efficient approach to creating a successful cybersecurity awareness and training program, Rege (2020) further stated that the NIST framework lays the necessary foundation for creating programs that produce factual changes in cybersecurity.

Chowdhury and Gkioulos (2021) state that training programs can be evaluated for comprehensiveness before application whereas the evaluation on the effectiveness of the program can only be done after the training sessions have been completed (Chowdhury & Gkioulos, 2021) (S7), the statistical data on breaches before and after the training is one technique of evaluation; another method is to conduct experiments to test employee preparedness and capacity to detect and report attacks. The effectiveness of a cybersecurity training program can be ensured by making sure the training meets the requirements such as; (i) having training content that is appropriate for the target audience, (ii) content must be in line with the skills aimed to be developed, (iii) training must make use of hands-on exercises to develop practical abilities that assure trainees can deal with real-life problems, (iv) the program should reach the broadest possible audience, and (v) the program should have good cost or performance characteristics for long-term sustainability.

Zhang (2021)highlighted five issues that affect the effectiveness of cybersecurity and training programs, issues include (i) Employees feel bored by training methods that make use of inspirational videos which is then followed by answering multi-choice questions, employees do not pay attention, (ii)Lack of rewards and incentives results to lack of interest and motivation to participate in the program, (iii) programs that are not in line with employees specific organisation's security awareness needs results in lack of interest, (iv) learning styles and employees needs are not met by the programs, (v) Ongoing update and revision of training program and feedback from trainees are not in place (Zhang et al., 2021)(S30).

Organisations should not only focus on providing security training to their employees but a focus should also be given to creating and maintain a culture of security awareness (Zhang et al., 2021) (S30).

## 4.4 Reviewing the themes

This section is concerned with validating the themes and investigating whether they are adequate. The review of the themes aims to aid the refining of the themes if necessary. The purpose of reviewing the themes is to assist in the refinement of the themes if necessary. Internal homogeneity and external heterogeneity will be assessed, and this will serve as the foundation for judging the themes.

### 4.4.1 Internal homogeneity

Internal homogeneity is a criterion concerned with the degree to which data belonging to a specific category or code holds together in a meaningful way(Patton, 2015).The internal homogeneity will be evaluated to determine the consistency of the data and whether the data has meaningful supporting data.

The frequency of the number of codes in each theme for methods of building cybersecurity knowledge is indicated in Table 4-18 and graphically presented in Figure 4-2 below.

UNIVERSITY OF JOHANNESBURG

**Table 4-17: Summary 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 | 25.71% |
| S1, S2, S8, S18, S20 | Unauthorised access | 6 | 8.57% |
| S1, S2, S8, S14, S25, S29 | Negligence | 6 | 8.57% |
| S2, S3, S4, S7, S8, S10, S20, S22, S24, S25, S26, S29, S30 | Social engineering | 13 | 18.57% |
| S1, S4, S7, S8, S11, S24 | Malicious insider | 6 | 8.57% |
| S2, S4, S7, S8, S10, S15, S20, S24, S25, S30 | Malware/ransomware | 10 | 14.29% |
| S4, S8, S10, S20, S23, S25 | Stolen credentials | 6 | 8.57% |
| S11, S14, S15, S23, S29 | Denial of service | 5 | 7.14% |

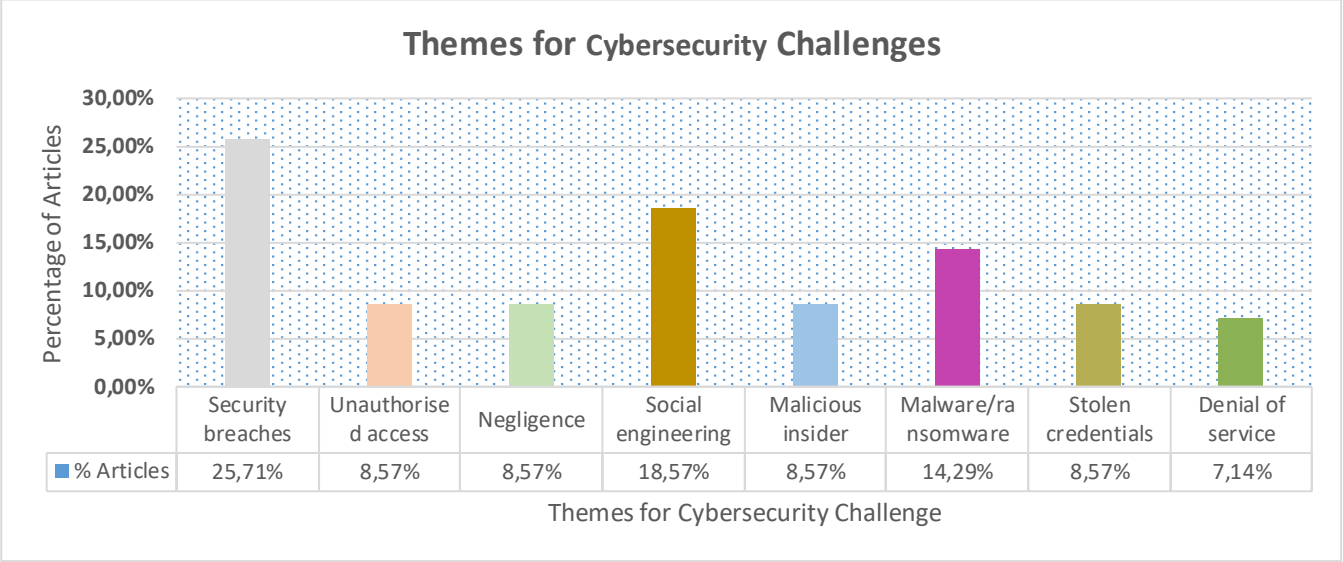


**Figure 4-1: Percentage of articles per the theme.**

In evaluating the Internal homogeneity for cybersecurity challenges, the summary of theme and frequency of codes presented in Table 4-17 and Figure 4-2 above were assessed, it was evident that the theme "security breaches" had more codes appearance of 18 and it constitute 24% of articles, this indicates that the codes are holding together in a meaningful way. The frequency of code appearance was then followed by the social engineering and malware/ransomware themes of which constituted 17% and 16% respectively. Themes unauthorised access and negligence had equal code frequency appearance of seven and representing 9% of articles each. Stolen credentials have a frequency of six and constitute 8% of articles, denial of service appeared as the theme with less frequency of codes appearances and constituting 7% of articles.

The frequency of the number of codes in each theme for methods of building cybersecurity knowledge is indicated in Table 4-18 and graphically presented in Figure 4-2 below.

**Table 4-18: 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 | 26.67% |
| S2, S10, S22, S23, S25, S26, S28, S30 | Cybersecurity awareness | 8 | 26.67% |
| S3, S29 | Cybersecurity culture | 2 | 6.67% |
| S1, S7, S10, S11, S14, S15, S18, S20, S24, S25, S26, S30 | Cybersecurity training | 12 | 40% |

UNIVERSITY OF JOHANNESBURG

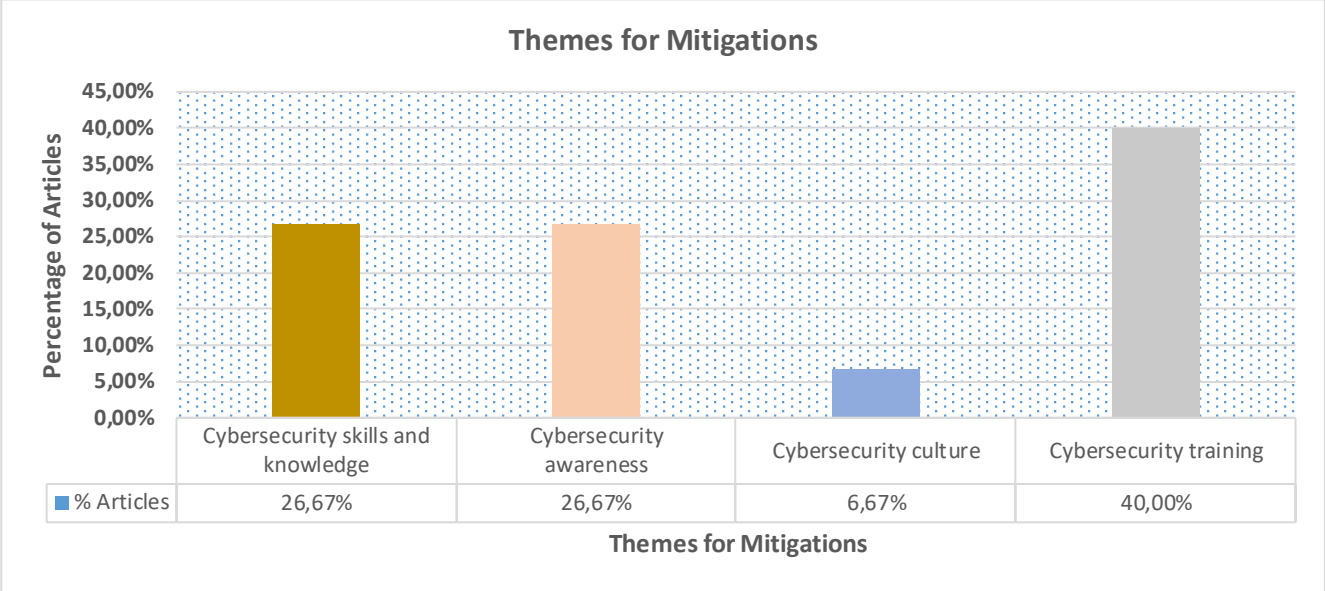


**Figure 4-2: Percentage of articles per the theme**

In evaluating the Internal homogeneity for methods of building cybersecurity knowledge, the summary of theme and frequency of codes presented in Table 4-18 and Figure 4-2 above were assessed, it was evident that the theme "cybersecurity training" had more codes appearance of 12 and it constitutes 40% of articles, this indicates that the codes are holding together in a meaningful way. The frequency of code appearance was then followed by the cybersecurity skills and knowledge and cybersecurity awareness themes of which had an equal code frequency appearance of eight and representing 27% of articles each. Cybersecurity culture appeared as the theme with less frequency of codes appearances and constituting 7% of articles.

### 4.4.2 External heterogeneity

External heterogeneity is a criterion for determining the degree to which differences between categories are clear and bold (Patton, 2015). The presence of a high number of unassignable or overlapping data items indicates that the category system has a fundamental flaw(Patton, 2015).

The distinctiveness of the themes was assessed, as well as whether there were any overlaps of similar ideas amongst them, to determine their heterogeneity. Although the themes may be related, it is necessary to be able to distinguish between them(Braun & Clarke, 2006b). The current themes' method consists of two steps: first, revisit the extracted codes that make up the theme to determine if the pattern is consistent, and second, if the chosen theme is consistent and the supporting codes create a coherent pattern, proceed to the next stage. If this is not the case, the themes must be reviewed and maybe changed or removed from the data.(Braun & Clarke, 2006b)

In evaluating the external heterogeneity, the chosen themes were found to be consistent with the supporting codes creating a unified pattern. The theme "cybersecurity culture" appeared less coherent as compared to the other themes.

UNIVERSITY OF JOHANNESBURG

## 4.5 Reporting

Reporting on the themes will follow, paragraphs will be extracted from the studies and paraphrased for the authenticity of the codes. The reporting and discussion on the theme will respond to some parts of the research question.

### 4.5.1 Reporting on the knowledge required to mitigate cybersecurity threats

This section is the write up on the knowledge required to mitigate cybersecurity threats identified from the 21 collected studies from which a systematic literature review was used. The studies were analysed using thematic analysis. The identified challenges are the blocks of knowledge that employees must be made aware of.

Cybersecurity is the protection of internet-connected systems that includes hardware, software, and data from cyberattacks whereas a cybersecurity incident is defined as a maliciously launched instruction from cyberspace to cause harm to a certain sector, company, industry, or entity.(Alabi et al., 2021). The water sector is one of the most critical infrastructures, identifying and controlling cyber threats to its facilities is critical to ensuring a reliable and secure supply of water(Shapira et al., 2021). According to Alabi(2021) cybersecurity has been identified as a major issue in the water sector. Industry entities and stakeholders must therefore devote significant attention and resources to assure cybersecurity preparedness and feedback from both a governance and technological standpoint.

Figure 4-3 below is the summary of different types of cyberattacks that are prevalent in critical infrastructure. The different types of cyberattacks were identified by analysing the 21 articles. The common types of cybersecurity threats indicated in each study were highlighted and allocated a single digit per study. Categorising the data as illustrated in Figure 4-3 enabled the recognition of literature research direction in terms of the common types of cybersecurity challenges and threats. Threats identified per study are graphically represented below.

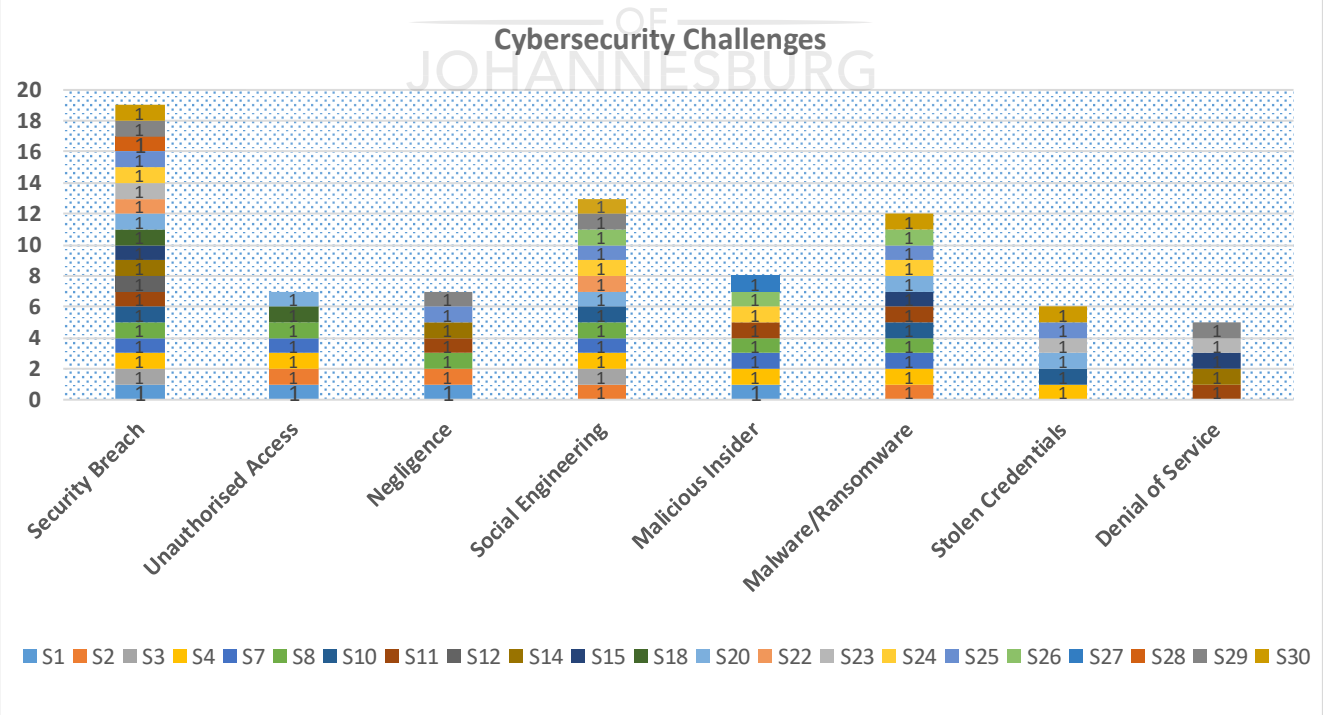


**Figure 4-3: Types of cybersecurity threats per study**

UNIVERSITY OF JOHANNESBURG

### 4.5.2 Reporting on methods of building cybersecurity knowledge

This section is the write up on the methods for building cybersecurity knowledge as identified from the 21 collected studies from which a systematic literature review was used. The studies were analysed using thematic analysis. The identified methods are the building blocks from which cybersecurity knowledge can be built to enable employees to protect the critical infrastructure.

Figure 4-4 below is the summary of different types of methods that can be used to build the cybersecurity knowledge of employees. These methods were identified by analysing the 21 articles. The common methods of building cybersecurity knowledge were allocated a single digit per study. Categorising the data as illustrated in Figure 4-4enabled the recognition of literature research direction in terms of the common methods for building cybersecurity knowledge. The methods identified per study are graphically represented below.

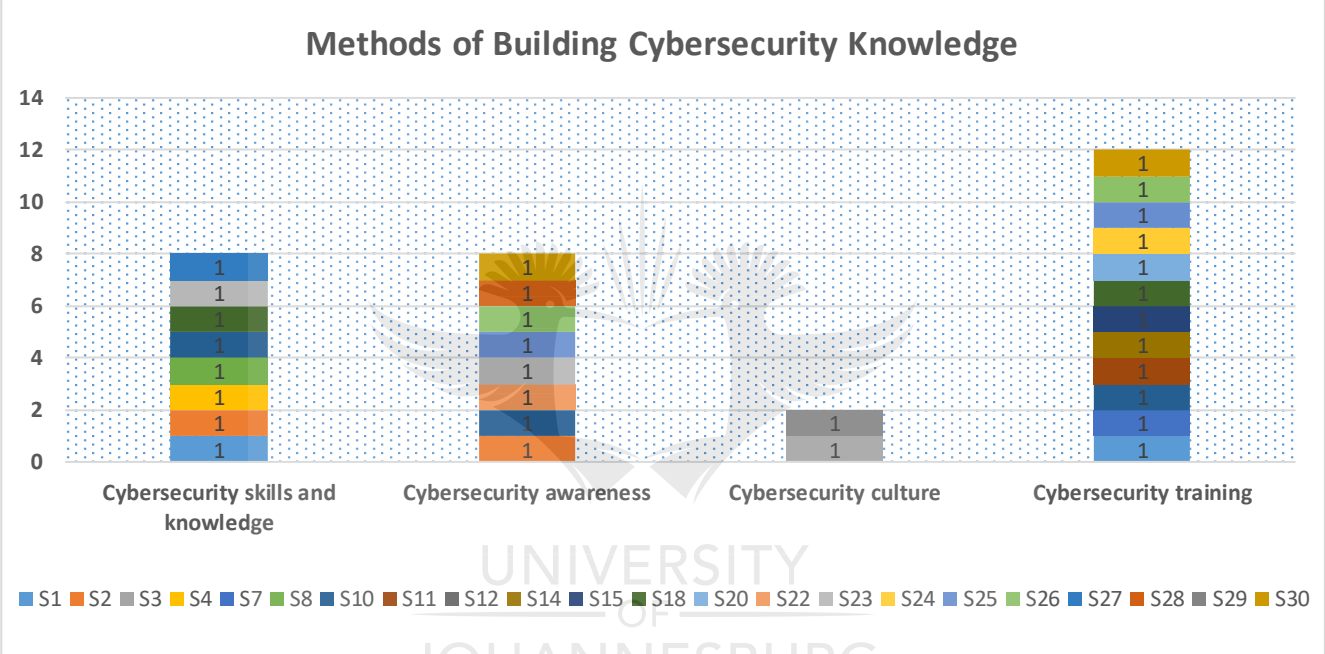


**Figure 4-4: Methods of building cybersecurity knowledge per study**

The summary section below gives a high-level summary of the findings from the data analysis.

### 4.5.3 Framework for identifying employee cybersecurity knowledge required

To mitigate the cyberthreats, a conceptual framework to identify the cybersecurity knowledge required will be developed through a process of reviewing and analysing some selected information related to cybersecurity challenges and mitigation methods. Several cybersecurity threats together with the proposed methods of mitigations and models were presented in the collected data for mitigating various cyberthreats. The conceptual framework will however focus on showing the key concepts for minimizing cyber threats and the hypothesized relationship between the cyber threats and mitigation methods. The output from the framework will be the identification of cybersecurity knowledge required. The foundation of the framework emerged from the existing knowledge discovered from the analysed literature.

UNIVERSITY OF JOHANNESBURG

Responding to security threats necessitates cybersecurity skill and knowledge training. It is critical to teach all employees and organizational leaders cybersecurity skills so that they can better guard against and respond to cyber threats (Adams, M. and Makramalla, 2015). The detection and reaction to critical circumstances is a crucial component that companies should prioritize. These measures have the potential to dramatically decrease losses associated with cyber security breaches(Mishra et al., 2016). Employees' understanding of information security is seen as a protective element whereas lack of awareness is about dangers to which employees may be exposed to if the risk is not properly identified or detected in advance (Nagarajan et al., 2012).

Following the rigorous data analysis and the interpretation of results, the framework depicted in Figure 4-6 was developed based on literature on cybersecurity from which data analysis and synthesis was conducted. The 21 literature studies demonstrated various ways on how cybersecurity knowledge can be built. Employee cybersecurity knowledge can be accomplished through analysis of the types of threats together with cybersecurity practices (mitigations). The outcome of each control measure can be categorised at an individual level or organisational level. The identified cyber threats reflect the knowledge that a general should have, whereas the mitigations indicate the methodologies and procedures by which such knowledge may be created.

The frameworks begin by defining the eight types of cybersecurity risks, followed by mitigation strategies for dealing with such attacks. The authors in the 21 literature studies provided several approaches and strategies for mitigating various cybersecurity risks. To deal with such risks, mitigations such as cybersecurity knowledge and skills, cybersecurity awareness, and cybersecurity training were proposed. The strategies for developing knowledge to deal with various sorts of dangers were provided at both the individual and organizational levels.

The procedure depicted in Figure 4-6 consists of the following steps:

- Types of cyberthreats: Eight common types of threats were identified from data synthesis and analysis.
- Mitigations: Four mitigations measures for reducing successful attacks were identified.
- Building knowledge at individual level: Minimal skills required by individuals to curb cyber risk were identified and summarised, with few examples listed.
- 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.

A high-level approach leading towards building and identifying the cybersecurity knowledge required for a general employee is depicted in Figure 4-5 where the basic Input Process Output (IPO) model was followed in building the framework illustrated in Figure 4-6.

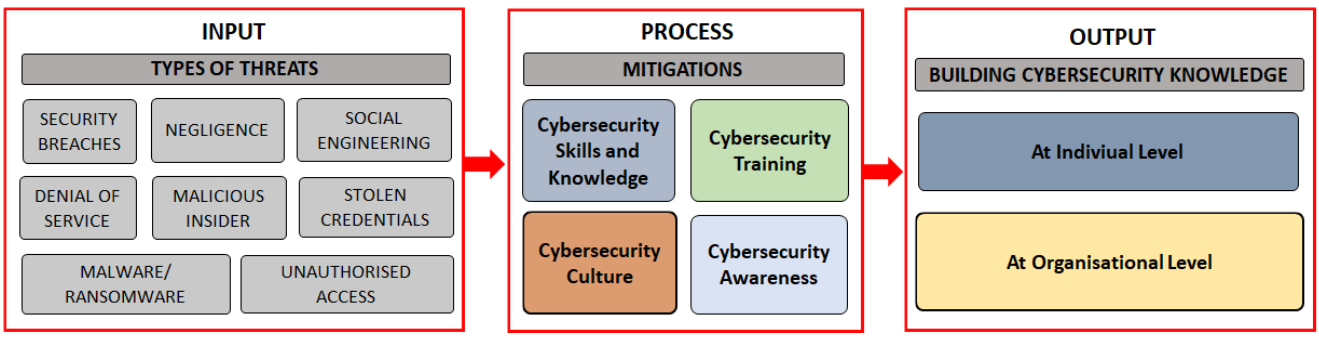


**Figure 4-5: IPO Model for Building Cybersecurity Knowledge**

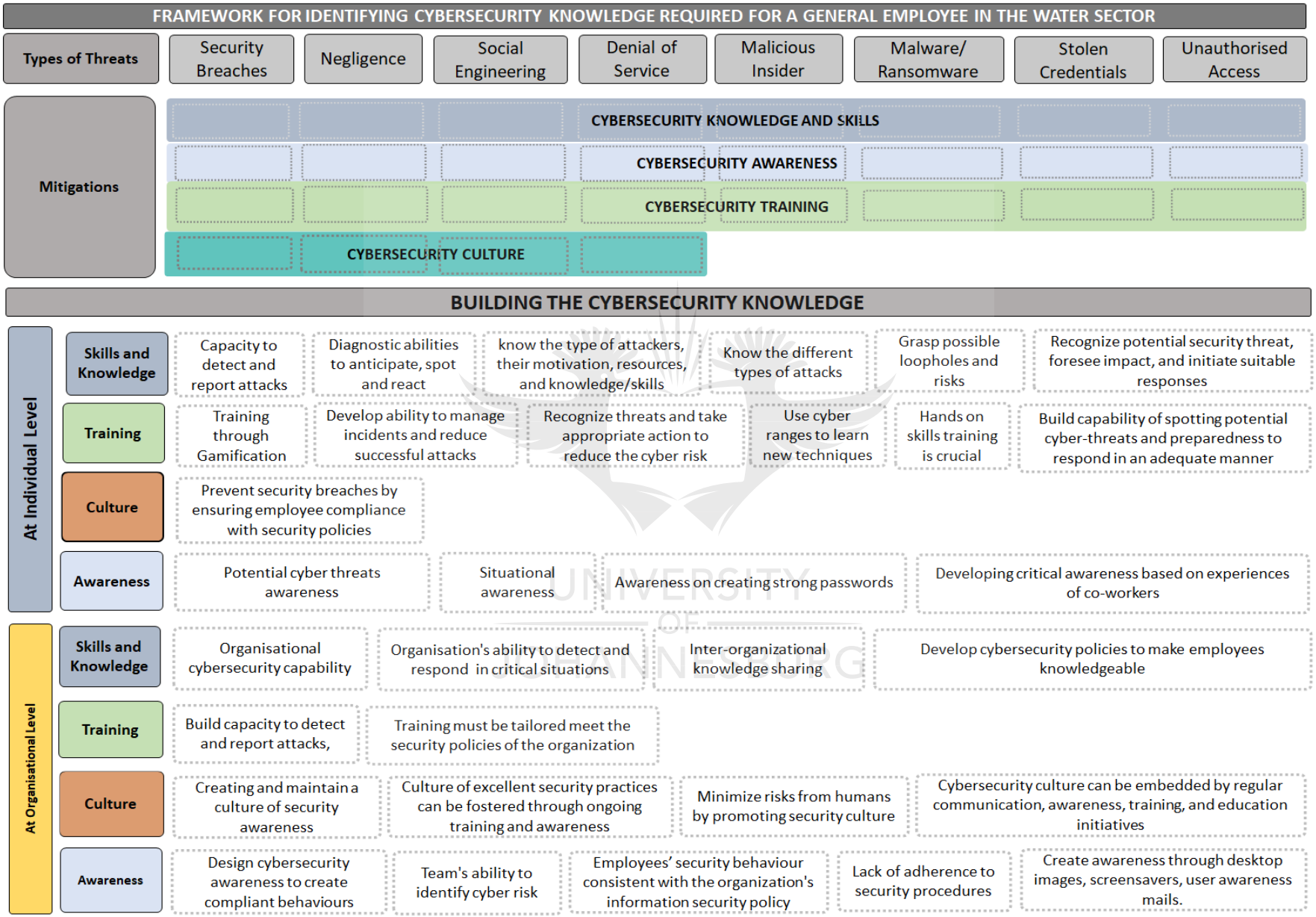


**Figure 4-6:Framework for identifying cybersecurity knowledge**

The literature studies gathered agree that a general employee in the water sector should be knowledgeable about the eight types of cybersecurity threats as identified as (i) security breaches, (ii) employee negligence, (iii) social engineering, (iv) denial of service, (v) malicious insider, (vi) malware/ransomware, (vii) stolen credentials and (viii) unauthorised access. The protection of critical infrastructure can be achieved by building the knowledge of employees through injecting mitigations such as (1) cybersecurity knowledge and skills where at an individual level: employees develop the capacity to detect and report cyberattacks, have the ability to diagnose in order to anticipate, spot and react to cyberattacks. It is important that employees are knowledgeable on the different types of attackers, their motivation, resources and skills, this further assist in gasping possible loopholes and risks. The other key element in 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 a joint organisational cybersecurity capability of the staff which include the ability to detect and respond in critical situations, sharing of knowledge amongst employees, and the development of policies aimed at making employees knowledgeable.

The second mitigation measure that leads towards building cybersecurity knowledge is (2) cybersecurity training. At an individual level, employees can gain valuable skills through developing abilities to manage incidents and reducing successful attacks. Through training, individuals can develop abilities to recognise threats and take appropriate action. The capability of spotting cyber threats 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 in such a way that it is tailored to meet the security policies of an organisation.

The third element in building cybersecurity knowledge is (3) cybersecurity culture. Cybersecurity culture should be indebted within organisations in order to prevent security breaches. This can be achieved by ensuring that a culture of security awareness is created and maintained within the organisation, fostering excellent security practices by through on-going training and awareness. Regular communication is important to maintain the culture of safe practices, this can be achieved through a number of initiatives that includes education and awareness.

The fourth and last key element for building the cybersecurity knowledge of employees is (4) cybersecurity awareness. At an individual level, employees can develop situational awareness that will enable them to be aware of potential cyberthreats. It is a good practice to create awareness on creating strong password 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 develop cybersecurity awareness to create compliant behaviours to enable team to have the ability to identify cyber risks. The security behaviour of employees must be in line with the organisation's security procedures. Ways to create employee awareness included the use of desktop images, screensavers and regularly feeding the users on awareness through emails.

## 4.6 Conclusion

The articles from the systematic literature review were analysed and synthesised in this chapter to help answer the research question. The 21 papers assisted in identifying the sorts of cybersecurity risks and problems, which were then utilized to build a framework, through analysis and synthesis. Thematic analysis methods such as analysing the data, developing initial codes, and constructing themes were shown to be beneficial. There are eight categories of cybersecurity risks identified, as well as four mitigation methods that may be used to combat these threats. Security breaches were recognized as the most prevalent cybersecurity threat for critical infrastructures, followed by social engineering and malware/ransomware.

UNIVERSITY OF JOHANNESBURG

# Chapter 5 : Conclusion

The last chapter of the research summarizes the study's general findings on defining a framework to identify the cybersecurity knowledge required for a general employee in the water sector. The chapter begins with a quick reminder of the research objective. This is followed by a description of the methodology followed before reporting on the finding. This chapter brings the study to a close by responding to the research questions given in the first chapter, therefore resolving the research problem and making recommendations for future research.

## 5.1 Introduction

In most, if not all, countries throughout the world, protecting critical infrastructure during natural and man-made disasters has become a top priority. The wave of successful cyberattacks on critical infrastructure has been growing in recent years. Identifying the cybersecurity expertise required of a general employee in the water sector is critical to the success of this dissertation. Many cyber-attacks have succeeded in defeating technical security systems by preying on human deficiencies in knowledge and skills and persuading insiders into unwittingly granting admission and access to sensitive information (Ani et al., 2016), for this reason, individuals are commonly seen as the weakest link in an organization's information security chain (Carlton et al., 2019), (Limba, T., Plėta, T., Agafonov, K. and Damkus, 2019), (Zhang et al., 2021). Due to the fact that technical operations personnel are frequently the weakest link in the security chain, they must be properly equipped and knowledgeable (Karampidis et al., 2019). “The water sector is one of the most critical infrastructures, and as such, identifying and managing cyber threats on the water sector’s facilities is crucial to providing a continuous and safe supply of water” (Shapira et al., 2021). The objective of this research is to:

- Develop approaches to follow in building the cybersecurity knowledge and awareness for a typical employee, to urge cybersecurity culture within organizations in the water sector.

A systematic literature review was the methodology employed. Search strategies were developed by using the PRISMA (Preferred Reporting Items for Systematic review and Meta-Analysis) guidelines as outlined by Liberati (2009). The inclusion and exclusion criteria were developed in line with the PRISMA guidelines to conduct the systematic literature review with consistency and transparency. Six electronic data bases were used together with the search strategy and the inclusion/exclusion criteria to extract data from the databases. These data bases include IEEE, Emerald Insight, Engineering Village, Wiley and Science Direct. A total of 2013 literature studies were obtained from these databases and were reduced to a total of 21 literature studies by following a rigorous screening process. The PRISMA diagram was then used to report on the number of documents removed and those included for analysis and synthesis as presented in chapter 4.

In conducting the systematic literature review, several factors for consideration in reducing successful cyberattacks were explored and presented from the identified and retrieved peer reviewed industry published articles. The identified threats and ways to mitigate such threats were summarised and presented. Many of the identified literature focused on training of personnel as a key aspect in reducing successful attacks to critical infrastructure.

The research protocol was adopted in advance to ensure the process of selecting the literature documents was unbiased. The research protocol also helped in defining the research question. The success of this systematic

literature review was subject to succeeding in carefully following the review protocol. The key search terms were standardised throughout the different databases to ensure consistency. Journals, books, magazines and conference papers were used to ensure a good systematic literature review

## 5.2 Summary of findings

The aim of this research is to develop approaches to follow in building the cybersecurity knowledge and awareness for a typical employee, to urge cybersecurity culture within organizations in the water sector. According to the findings of this study, employees are the weakest link in the organization's cybersecurity chain, as a result, it is vital for organizations to take appropriate steps to strengthen employee capability gaps in order to bridge the security risk gap. Employees that are aware of the vulnerabilities will be able to distinguish possible security risks, predict their impact, and take appropriate action. A research question was posed with the goal of addressing the research aim. The following is the research question:

***What knowledge is essential for employees to urge cybersecurity culture and awareness in the water sector's critical infrastructures?***

Cyberattacks on critical water infrastructure are becoming increasingly common, threatening service delivery. The acquired various forms of cyber risks were identified as the minimal knowledge/competency that a typical general employee in the water sector should have in order to limit successful assaults on critical water infrastructure. Data breaches, social engineering (phishing attacks), employee negligence, malicious insider, malware/ransomware, unauthorised access, stolen credentials, and denial of service assaults were recognized as the eight risks that every general employee should be aware of as depicted in Figure 5-1 below.

UNIVERSITY OF JOHANNESBURG

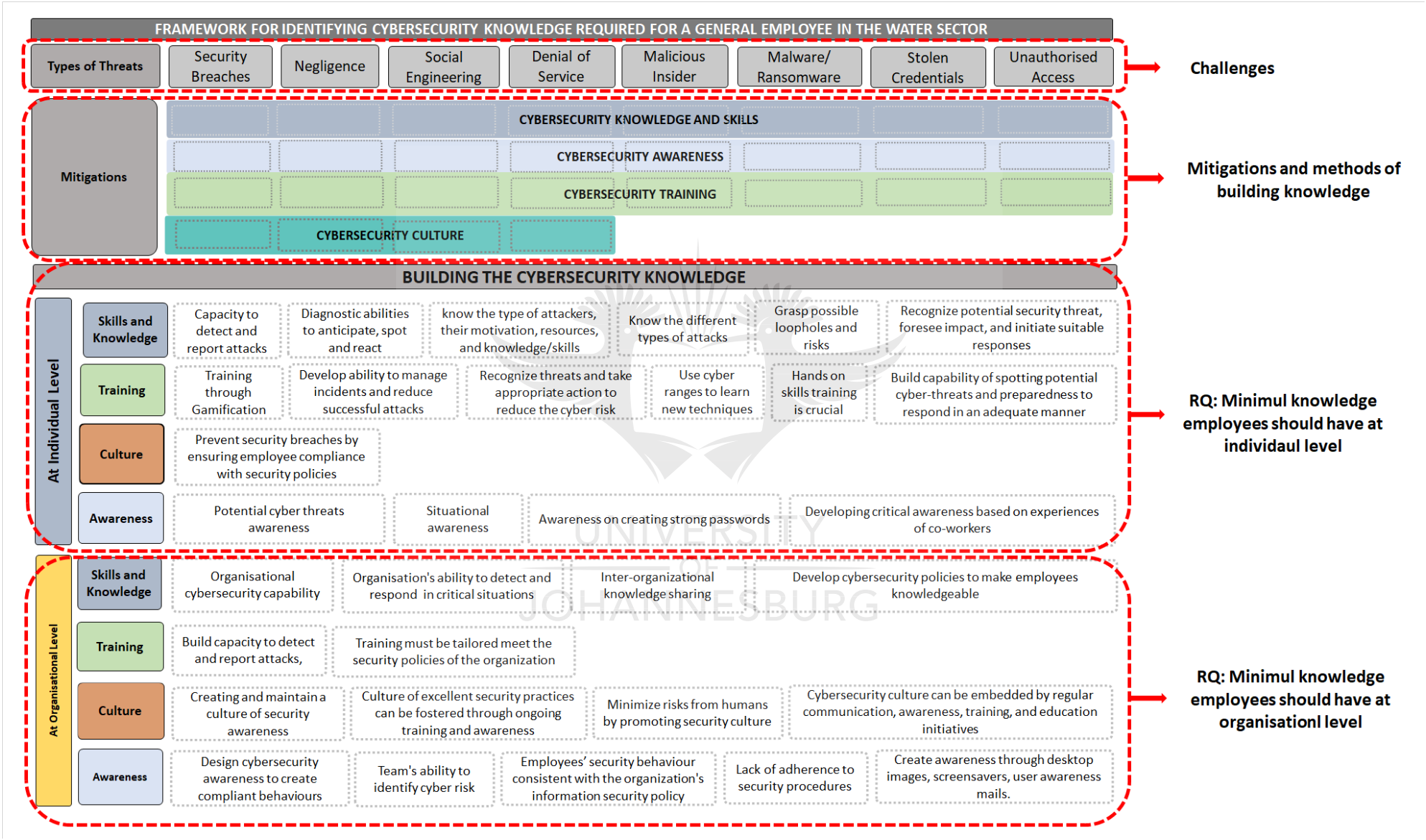


**Figure 5-1: Framework for identifying cybersecurity knowledge**

Four mitigation methods were identified for both the individual and organizational levels to mitigate the vulnerabilities and hazards indicated as the minimal knowledge or capabilities as illustrated in Figure 5-1. These methods are, cybersecurity skills and knowledge, cybersecurity training, cybersecurity culture and cybersecurity awareness. An organization's attitude toward cyber security is frequently reflected in the knowledge and skills of its personnel (Ani et al., 2016). Knowledge and skills can reduce human mistake due to a lack of cybersecurity knowledge and awareness which is one of the major causes of cyber-incidents, thus cybersecurity awareness in a company is important (Prins et al., 2020).

Cybersecurity skills and knowledge together with cybersecurity training may improve the overall culture and awareness at an individual and organisational levels. The cybersecurity culture dimension necessitates that the an organisation and each individual have a comprehensive grasp of all security measures that can be utilized within the organization to try to improve cybersecurity, this includes managing employees and giving a clear description of the abilities that each organization member must achieve (Limba, T., Plėta, T., Agafonov, K. and Damkus, 2019). Other variables, such as corporate culture, have been discovered to influence individuals to comply with suggested information security behaviour at the organizational level (AlMindeel & Martins, 2021).

## 5.3 Future studies

The study's goal was met by concluding that a general employee in the water sector should be exposed to the eight types of cyberthreats, which are data breaches, social engineering (phishing attacks), employee negligence, malicious insider, malware/ransomware, unauthorised access, stolen credentials, and denial of service attacks. Cybersecurity culture can be urged by implementing cybersecurity knowledge and skills training. As highlighted in chapter 1, This study will also serve as the foundation for future work, which will involve the development of the theoretical framework through feedback from water industry specialists. The finalized framework will guide the creation of instructional materials that will educate personnel in the industry on how to better safeguard infrastructure and foster a cybersecurity culture in the sector.

UNIVERSITY OF JOHANNESBURG

## References


Adams, M. and 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

Alabi, M., Telukdarie, A., & Rensburg, N. J. Van. (2021). *Cybersecurity And Water Utilities : Factors For Influencing Effective Cybersecurity Implementation In Water Sector Cybersecurity And Water Utilities : Factors For Influencing Effective Cybersecurity Implementation In Water Sector*. *March*.

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

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

Ani, P., He, H., & Tiwari, A. (2016). Human Capability Evaluation Approach for Cyber Security in Critical Industrial Infrastructure. *Advances in Human Factors in Cyebrsecurity*, *Vol 501*, 267–277. https://doi.org/10.1007/978-3-319-41932-9

Bode, M. A., Oluwadare, S. A., Alese, B. K., & Thompson, A. F. B. (2015). Risk analysis in cyber situation awareness using Bayesian approach. *2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2015*, *June*. https://doi.org/10.1109/CyberSA.2015.7166119

Boell, S. K., & Cecez-Kecmanovic, D. (2015). On being "systematic" in literature reviews in IS. *Journal of Information Technology*, *30*(2), 161–173. https://doi.org/10.1057/jit.2014.26

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

Braun, V., & Clarke, V. (2006b). *Using thematic analysis in psychology*.

Braun, V., & Clarke, V. (2012). *Thematic analysis*. *2*. https://doi.org/10.1037/13620-004

Briner, R. B., & Denyer, D. (2012). Systematic Review and Evidence Synthesis as a Practice and Scholarship Tool. *The Oxford Handbook of Evidence-Based Management*. https://doi.org/10.1093/oxfordhb/9780199763986.013.0007

Burghouwt, P., Maris, M., van Peski, S., Luiijf, E., van de Voorde, I., & Spruit, M. (2017). Cyber targets water management. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10242 LNCS*, 38–49. https://doi.org/10.1007/978-3-319-71368-7_4

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

Catota, F. E., Granger Morgan, M., & Sicker, D. C. (2019). Cybersecurity education in a developing nation: The Ecuadorian environment. *Journal of Cybersecurity*, *5*(1), 1–19. https://doi.org/10.1093/cybsec/tyz001

Centre for Reviews and Dissemination. (2009). *CRD's guidance for undertaking reviews in health care*. Centre for Reviews and Dissermaton, University of York.

Chileshe, G., & Heerden, R. Van. (2012). SCADA systems in South Africa and their vulnerabilities. *7th International Conference on Information Warfare and Security, ICIW 2012*, 90–97.

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

Clark, R. M., Hakim, S., & Ostfeld, A. (2011). Handbook of Water and Wastewater Systems Protection. *Handbook of Water and Wastewater Systems Protection*, 1–25. https://doi.org/10.1007/978-1-4614-0189-6

Da¸s, R., & Gündüz, M. Z. (2019). Analysis of Cyber-Attacks in IoT-based Critical Infrastructures. *International Journal of Information Security Science*, *8*(4), 122–133.

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, SAI 2016*, 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

Domínguez, M., Prada, M. A., Reguera, P., Fuertes, J. J., Alonso, S., & Morán, A. (2017). *Cybersecurity training in control systems using real equipment*. *50*(1), 12179–12184. https://doi.org/10.1016/j.ifacol.2017.08.2151

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. *ICISSP 2021 - Proceedings of the 7th International Conference on Information Systems Security and Privacy*, *January*, 702–713. https://doi.org/10.5220/0010393107020713

Fereday, J. (2006). *Demonstrating Rigor Using Thematic Analysis : A Hybrid Approach of Inductive and Deductive Coding and Theme Development*. 80–92. https://doi.org/10.1177/160940690600500107

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

Flaus, J. (2019). Vulnerabilities of ICS. *Cybersecurity of Industrial Systems*, 121–139. https://doi.org/10.1002/9781119644538.ch5

Ganann, R., Ciliska, D., & Thomas, H. (2010). *Expediting systematic reviews : methods and implications of rapid reviews*. 1–10.

Geers, K. (2009). The cyber threat to national critical infrastructures: Beyond theory. *Information Security Journal*, *18*(1), 1–7. https://doi.org/10.1080/19393550802676097

Green, S. (2008). Cochrane Handbook for Systematic Reviews of Interventions. In *Cochrane Handbook for Systematic Reviews of Interventions*. https://doi.org/10.1002/9781119536604

Haddaway, N. R., Woodcock, P., Macura, B., & Collins, A. (2015). Making literature reviews more reliable through application of lessons from systematic reviews. *Conservation Biology*, *29*(6), 1596–1605. https://doi.org/10.1111/cobi.12541

Ham-baloyi, W., & Jordan, P. (2015). ScienceDirect Systematic review as a research method in post- graduate nursing education. *Health SA Gesondheid*, *21*(0), 120–128. https://doi.org/10.1016/j.hsag.2015.08.002

He, W., Ash, I., Anwar, M., Li, L., Yuan, X., Xu, L., & Tian, X. (2019). Improving employees' intellectual capacity for cybersecurity through evidence-based malware training. *Journal of Intellectual Capital*, *21*(2), 203–213. https://doi.org/10.1108/JIC-05-2019-0112

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

UNIVERSITY OF JOHANNESBURG

http://onlinelibrary.wiley.com/doi/10.1002/9780470712184.fmatter/summary

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

Josette Bettany-Saltikov. (2012). How to do a Systematic Literature Review in Nursing. A Step-by-Step Guide. In *Nurse Education in Practice* (Vol. 13, Issue 3). https://doi.org/10.1016/j.nepr.2012.12.004

Kamioka, H. (2019). Preferred reporting items for systematic review and meta-analysis protocols (prisma-p) 2015 statement. *Japanese Pharmacology and Therapeutics*, *47*(8), 1177–1185.

Karabacak, B., Yildirim, S. O., & Baykal, N. (2016). *Regulatory approaches for cyber security of critical infrastructures : The case of Turkey Regulatory approaches for cyber security of critical infrastructures : The case of Turkey Bilge Karabacak *, Sevgi Oz*. *32*, 526–539.

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, CAMAD*, *2019-Septe*. https://doi.org/10.1109/CAMAD.2019.8858454

Keupp, M. M., Palmié, M., & Gassmann, O. (2012). *The Strategic Management of Innovation : 14*, 367–390. https://doi.org/10.1111/j.1468-2370.2011.00321.x

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

Kitchenham, B. (2004). A rare case of Erdheim-Chester disease in the breast. *Procedures for Performing Systematic Reviews*, *37*(1).

Kraus, S., Breier, M., & Dasí-Rodríguez, S. (2020). The art of crafting a systematic literature review in entrepreneurship research. *International Entrepreneurship and Management Journal*, *16*(3), 1023–1042. https://doi.org/10.1007/s11365-020-00635-4

Lee, S., Speight, J. G., Lee, S., & Speight, J. G. (2020). Water Systems. *ENVIRONMENTAL Technology Handbook*, 93–117. https://doi.org/10.1201/9780367813390-6

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. In *Journal of clinical epidemiology* (Vol. 62, Issue 10). https://doi.org/10.1016/j.jclinepi.2009.06.006

Limba, T., Plėta, T., Agafonov, K. and Damkus, M. (2019). Cyber Security Management Model For Critical Infrastructure Tadas. *Cyber Security Management Model for Critical Infrastructure.*

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, Euro S and PW 2020*, 448–453. https://doi.org/10.1109/EuroSPW51379.2020.00066

Malatji, M., Marnewick, A. L., & von Solms, S. (2021). Cybersecurity Policy and the Legislative Context of the Water and Wastewater Sector in South Africa. *Sustainability*, *13*(1), 291.

Malatji, M., Marnewick, A., & von Solms, S. (2020). Validation of a socio-technical management process for optimising cybersecurity practices. *Computers and Security*, *95*, 101846. https://doi.org/10.1016/j.cose.2020.101846

Mambile, C., & Mbogoro, P. E. (2020). Cybercrimes awareness, cyber laws and its practice in public sector tanzania. *International Journal of Advanced Technology and Engineering Exploration*, *7*(68), 119–126.

https://doi.org/10.19101/IJATEE.2020.762051

Mishra, S., Howles, T., Raj, R. K., Romanowski, C. J., Schneider, J., McNett, A., & Dates, D. J. (2016). A modular approach to teaching critical infrastructure protection concepts to engineering, technology and computing students. *Proceedings - Frontiers in Education Conference, FIE*, *2016-Novem*. https://doi.org/10.1109/FIE.2016.7757367

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, HST 2015*. 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*, *0123456789*. https://doi.org/10.1007/s11135-020-01059-6

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, CYBER 2012*, 256–262. https://doi.org/10.1109/CYBER.2012.6392562

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). *Thematic Analysis : Striving to Meet the Trustworthiness Criteria*. *16*, 1–13. https://doi.org/10.1177/1609406917733847

Noyes, J., Popay, J., Pearson, A., Hannes, K., & Booth, A. (2008). Qualitative Research and Cochrane Reviews. *Cochrane Handbook for Systematic Reviews of Interventions: Cochrane Book Series*, *October 2017*, 571–591. https://doi.org/10.1002/9780470712184.ch20

Panchal, K., & Damodaran, M. (2017). Computation of the flowfield in the vicinity of an electric vehicle platform. *Lecture Notes in Mechanical Engineering*, *2018*, 333–341. https://doi.org/10.1007/978-81-322-2743-4_32

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

Panguluri, S., Phillips, W., & Ellis, P. (2011). Handbook of Water and Wastewater Systems Protection. In *Handbook of Water and Wastewater Systems Protection*. https://doi.org/10.1007/978-1-4614-0189-6

Parker, A., & Brown, I. (2019). Skills requirements for cyber security professionals: A content analysis of job descriptions in South Africa. In *Communications in Computer and Information Science* (Vol. 973). Springer International Publishing. https://doi.org/10.1007/978-3-030-11407-7_13

Patton, M. (2015). *Qualitative Research and Evaluation Methods (4th Edition)* (Vol. 148).

Paulsen, C., McDuffie, E., Newhouse, W., & Toth, P. (2012). NICE: Creating a cybersecurity workforce and aware public. *IEEE Security and Privacy*, *10*(3), 76–79. https://doi.org/10.1109/MSP.2012.73

Petticrew, M., & Roberts, H. (2008). Systematic Reviews in the Social Sciences: A Practical Guide. In *Systematic Reviews in the Social Sciences: A Practical Guide*. https://doi.org/10.1002/9780470754887

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

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, ISEC 2020*, 1–6. https://doi.org/10.1109/ISEC49744.2020.9280596

Shapira, N., Ayalon, O., Ostfeld, A., Asce, F., Farber, Y., Housh, M., & Asce, M. (2021). *Cybersecurity in Water*

*Sector : Stakeholders Perspective*. *147*(8), 1–15. https://doi.org/10.1061/(ASCE)WR.1943-5452.0001400

South Africa Operational Risk Report. (2021). In *Fitch Solutions Risk Reports; London* (Vol. 54, Issue 4). https://search.proquest.com/reports/south-africa-operational-risk-report-q2-2021/docview/2495835381/se-2?accountid=13425

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. https://doi.org/10.1016/j.infsof.2009.11.006

Tawfik, G. M., Dila, K. A. S., Mohamed, M. Y. F., Tam, D. N. H., Kien, N. D., Ahmed, A. M., & Huy, N. T. (2019). A step by step guide for conducting a systematic review and meta-analysis with simulation data. *Tropical Medicine and Health*, *47*(1), 1–9. https://doi.org/10.1186/s41182-019-0165-6

Taylor, J. (2012). Doing Your Literature Review – Traditional and Systematic Techniques Jill K Jesson Doing Your Literature Review – Traditional and Systematic Techniques, LydiaMatheson Fiona MLacey. In *Nurse Researcher* (Vol. 19, Issue 4, pp. 45–45). https://doi.org/10.7748/nr.19.4.45.s7

Terry, B. G., Hayfield, N., Clarke, V., Braun, V., Terry, G., Hayfield, N., Clarke, V., & Braun, V. (2021). *In : The SAGE Handbook of Qualitative Research in Psychology Thematic Analysis*.

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, EAEEIE 2019 - Proceedings*, 2019–2022. https://doi.org/10.1109/EAEEIE46886.2019.9000440

Van Vuuren, J. J., Leenen, L., Phahlamohlaka, J., & Zaaiman, J. (2013). Development of a south african cybersecurity policy implementation framework. *8th International Conference on Information Warfare and Security, ICIW 2013*, *2010*, 106–115.

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, ASONAM 2018*, 774–781. https://doi.org/10.1109/ASONAM.2018.8508410

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.

Willis Towers Watson. (2019). *When it comes to cyber risk, businesses are missing the human touch - Willis Towers Watson*. 1–3.

World, S., World, S., & Oct, C. N. (2016). *Phil ' s Stock World : Cybersecurity ' s weakest link : humans*. 1–4.

Xiao, Y., & Watson, M. (2019). Guidance on Conducting a Systematic Literature Review. *Journal of Planning Education and Research*, *39*(1), 93–112. https://doi.org/10.1177/0739456X17723971

Zhang, Z. (Justin), 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

Zimmermann, V., & Renaud, K. (2019). Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human Computer Studies*, *131*(May), 169–187. https://doi.org/10.1016/j.ijhcs.2019.05.005

UNIVERSITY OF JOHANNESBURG

# APPENDIX A

## ProQuest literature online database

This database provides the researcher with a search tab and different tools that a searcher may use to enter the search terms and key phrases. The search strings in chapter 2 (Table 2-1) were entered in the search tab, the research results for string 1 returned 350 results of available articles whereas the research results for string 2 returned 312 results of available articles. The results were narrowed down by using the advanced search function. The advanced search options provided the option to use the Boolean search operators through adding rows of "OR", "AND" and "NOT" function on the search. Where key phrases were divided on each search tab. Also included was a function to search for key phrases in different categories with options such as anywhere, anywhere except full text, abstract, document full text, etc. The platform also provided the option to limit search to full text, peer reviewed, publication date and source type. The following steps illustrates the procedure followed in retrieving data from the search queries:

- Enter key search phrases in the advanced search tab.
- Separate each phrase with the "AND" operator.
- Select search literature in "Document text – FT".
- Select limit to "Full text" and "Peer reviewed".
- Select language "English".
- Select publication date for "all dates".
- Extract data to Endnote through downloading RIS files

**Table 1: ProQuest Literature Online data extraction summary**

| **Search string 1** | *Employees **AND** cybersecurity culture challenges **AND** Cybersecurity knowledge requirement **AND** Critical Infrastructure* | | | | | | |
|---|---|---|---|---|---|---|---|
| **Source type** | Journal Article | Conference paper | Book section | Article in Press | Magazine | Thesis | Total |
| **Results** | 349 | | | | 1 | | 350 |
| **Search string 2** | *Employees **AND** cybersecurity awareness problems **AND** Cybersecurity education and training **AND** Critical Infrastructure* | | | | | | |
| **Source type** | Journal Article | Conference paper | Book section | Article in Press | Magazine | Thesis | Total |
| **Results** | 310 | 1 | | | 1 | | 312 |

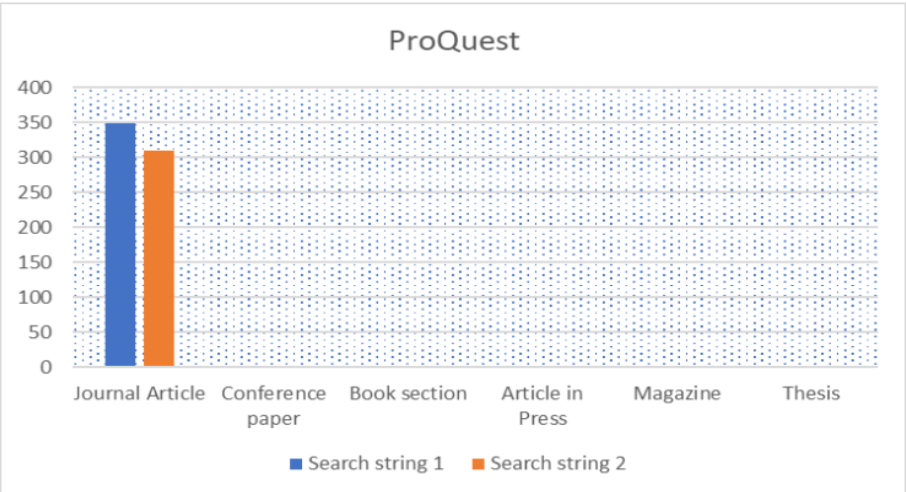


**Figure 1: Studies extracted from ProQuest.**

## IEEE Xplore database

On this database there is a search tab that a searcher may use to enter the search terms and key phrases. The search strings in chapter 2 (Table 2-1) were entered in the search tab, by making use of the advanced search function. The advanced search options provided the option to use the Boolean search operators through adding rows of "OR", "AND" and "NOT" function on the search. The search string 1 the research results returned 140 results of available articles whereas search string 2 returned 169 results of available articles. Also included was a function to search for key phrases in different categories with options such as All metadata, full text only, abstract, document title, etc. The following steps illustrates the procedure followed in retrieving data from the search queries:

- Enter key search phrases in the advanced search tab.
- Separate each phrase with the "AND" operator.
- Select search literature in "Full Text Only".
- Select data sources to "Conference, Books, Journals, Magazines and Early Access Articles".
- Specify year range "All years".
- Extract data to Endnote through downloading RIS files

**Table 2: IEEE Xplore data extraction summary**

| **Search string 1** | *Employees **AND** cybersecurity culture challenges **AND** Cybersecurity knowledge requirement **AND** Critical Infrastructure* | | | | | | |
|---|---|---|---|---|---|---|---|
| **Source type** | Journal Article | Conference paper | Book section | Article in Press | Magazine | Thesis | Total |
| **Results** | 23 | 55 | 42 | | 20 | | 140 |
| **Search string 2** | *Employees **AND** cybersecurity awareness problems **AND** Cybersecurity education and training **AND** Critical Infrastructure* | | | | | | |
| **Source type** | Journal Article | Conference paper | Book section | Article in Press | Magazine | Thesis | Total |
| **Results** | 20 | 86 | 46 | | 17 | | 169 |

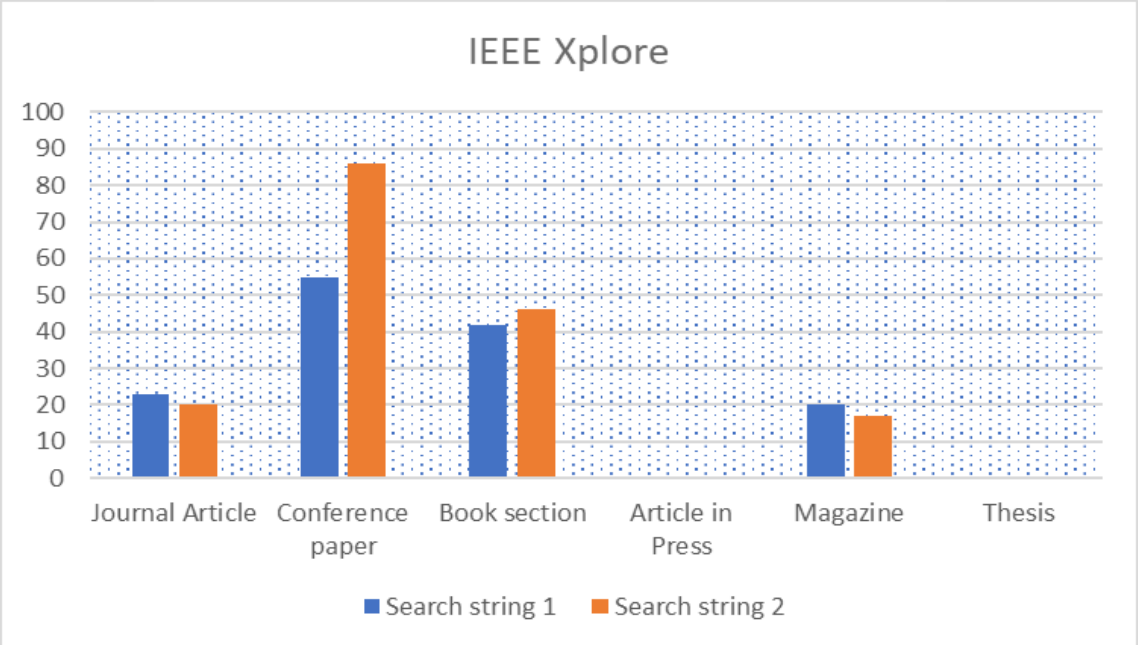


**Figure 2: Studies extracted from IEEE Xplore.**

## Emerald Insight online database

This database provides the researcher with a search tab and the option for advanced search. The search strings in chapter 2 (Table 2-1) were entered in the search tab, the search results for search string 1 returned 135 results of available articles while search string 2 returned 95 results of available articles. The advanced search options provided the option to use the Boolean search operators where the researcher can add rows of "OR", "AND" and "NOT" function on the search. Where key phrases were divided on each search tab. Also included was a function to search for key phrases in different categories with options such as all fields, title, abstract, contributor and DOI. The platform also provided the option to access all content or choose between only open access or only content I have access to. The following steps illustrates the procedure followed in retrieving data from the search queries:

- Enter key search phrases in the advanced search tab.
- Separate each phrase with the "AND" operator.
- Select search literature in "All fields".
- Select access to "Only documents I have access to".
- Select publication date for "All years".
- Extract data to Endnote through downloading RIS files

**Table 3: Emerald Insight data extraction summary**

| **Search string 1** | *Employees **AND** cybersecurity culture challenges **AND** Cybersecurity knowledge requirement **AND** Critical Infrastructure* | | | | | | |
|---|---|---|---|---|---|---|---|
| **Source type** | Journal Article | Conference paper | Book section | Article in Press | Magazine | Thesis | Total |
| **Results** | 131 | | 4 | | | | 135 |
| **Search string 2** | *Employees **AND** cybersecurity awareness problems **AND** Cybersecurity education and training **AND** Critical Infrastructure* | | | | | | |
| **Source type** | Journal Article | Conference paper | Book section | Article in Press | Magazine | Thesis | Total |
| **Results** | 90 | | 5 | | | | 95 |

UNIVERSITY OF JOHANNESBURG

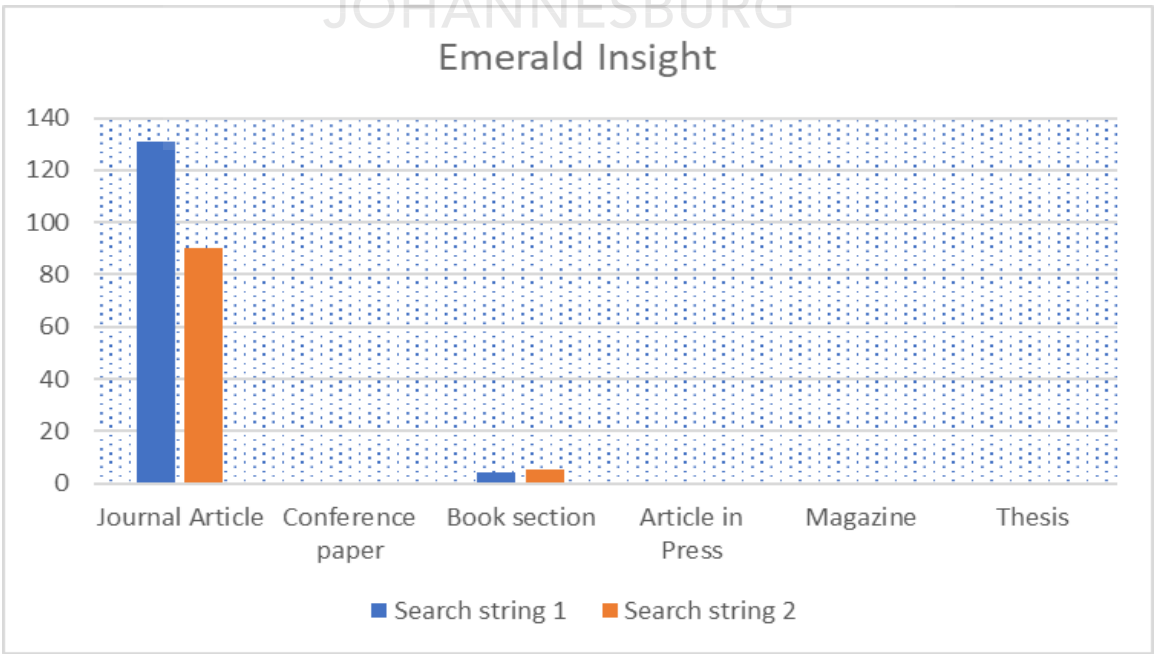


**Figure 3: Studies extracted from Emerald Insight.**

## Engineering Village online database

Engineering Village database provides the researcher with a search tab. The advanced search options provided to use the Boolean search operators where the researcher can add rows of "OR", "AND" and "NOT" function on the search tab where key phrases were divided on each search tab. The search strings in chapter 2 (Table 2-1) were entered in the search tab, the search results for search string 1 returned 208 results of available articles while search string 2 returned 247 results of available articles. Also included was a function to search for key phrases in different categories with options such as all fields, title, abstract, publisher and source title. The platform also provided the option to access all content or choose all databases or Complete index, Inspect Archive or Knovel. The following steps illustrates the procedure followed in retrieving data from the search queries:

- Enter key search phrases in the advanced search tab.
- Separate each phrase with the "AND" and "OR" operator.
- Select search literature in "Abstract".
- Select "All databases".
- Select data sources to "Conference, Books, Journals, Magazines and Journal Articles".
- Select publication date for "All years".
- Extract data to Endnote through downloading RIS files

**Table 4: Engineering Village data extraction summary**

| **Search string 1** | *Employees **OR** cybersecurity culture challenges **OR** Cybersecurity knowledge requirement **AND** Critical Infrastructure* | | | | | | |
|---|---|---|---|---|---|---|---|
| **Source type** | Journal Article | Conference paper | Book section | Article in Press | Magazine | Thesis | Total |
| **Results** | 49 | 144 | 6 | | | | 199 |
| **Search string 2** | *Employees **AND** cybersecurity awareness problems **AND** Cybersecurity education and training **AND** Critical Infrastructure* | | | | | | |
| **Source type** | Journal Article | Conference paper | Book section | Article in Press | Magazine | Thesis | Total |
| **Results** | 64 | 171 | 11 | 1 | | | 247 |

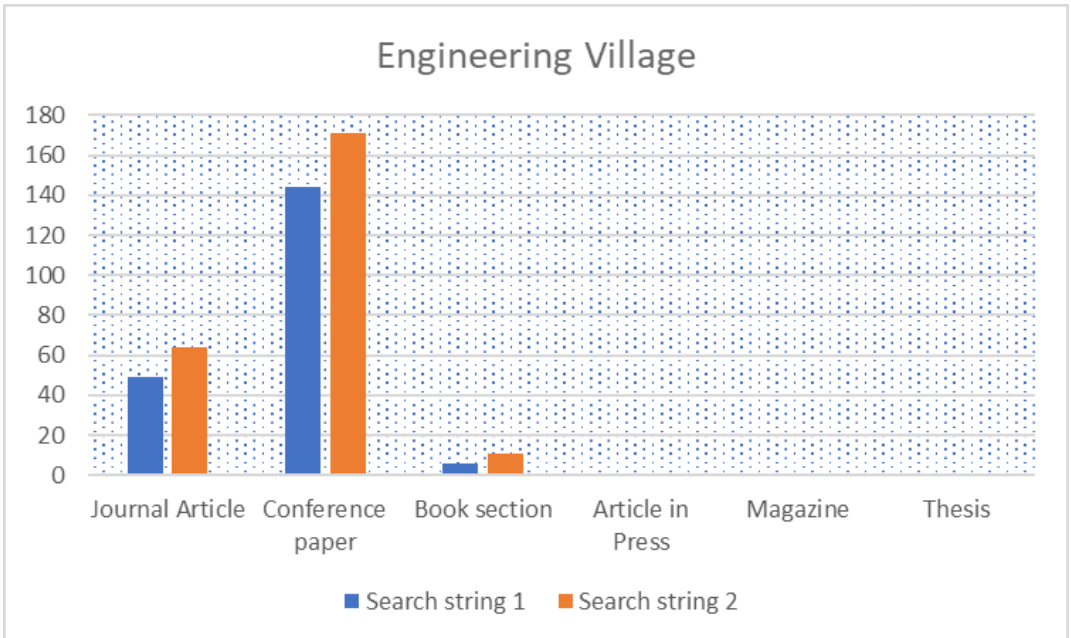


**Figure 4: Studies extracted from Engineering Village**

## Wiley Online library

On this database there is a search tab that a searcher may use to enter the search terms and key phrases. The search strings in chapter 2 (Table 2-1) were entered in the search tab, by making use of the refine research function where key search phrases can be entered separately with option to search the phrase anywhere, or using title, author, or keywords. The search string 1 the research results returned 56 results of available articles whereas search string 2 returned 50 results of available articles. Also included was a function to search for key phrases in different categories with options such as All metadata, full text only, abstract, document title, etc. The following steps illustrates the procedure followed in retrieving data from the search queries:

- Enter key search phrases separate tab.
- Refine search by selecting "anywhere, title, author or keywords".
- Add keyword as Cybersecurity.
- Select data sources to "conference, books, journals, magazines and early access articles".
- Specify publication date "All dates".
- Extract data to Endnote through downloading RIS files.

**Table 5: Wiley Online Library data extraction summary**

| **Search string 1** | *Employees **AND** cybersecurity culture challenges **AND** Cybersecurity knowledge requirement **AND** Critical Infrastructure* | | | | | | |
|---|---|---|---|---|---|---|---|
| **Source type** | Journal Article | Conference paper | Book section | Article in Press | Magazine | Thesis | Total |
| **Results** | 10 | | 46 | | | | 56 |
| **Search string 2** | *Employees **AND** cybersecurity awareness problems **AND** Cybersecurity education and training **AND** Critical Infrastructure* | | | | | | |
| **Source type** | Journal Article | Conference paper | Book section | Article in Press | Magazine | Thesis | Total |
| **Results** | 10 | | 40 | | | | 50 |

UNIVERSITY OF JOHANNESBURG

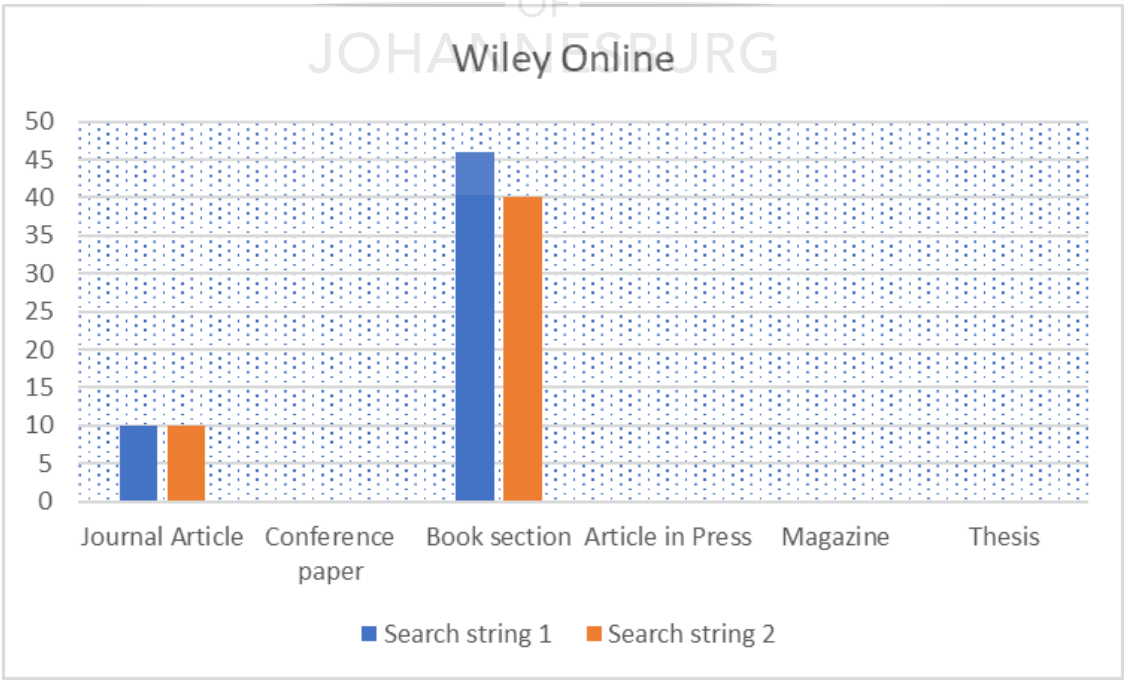


**Figure 5: Studies extracted from Wiley Online**

## ScienceDirect online database

On ScienceDirect the searcher enters the search terms and key phrases on the search tab. The search options do not provide the use the Boolean search operators, but the researcher can type “OR”, “AND” and “NOT” in between the key search phrases on the search tab. The search strings in chapter 2 (Table 2-1) were entered in the search tab, the search results for search string 1 returned 133 results of available articles while search string 2 returned 127 results of available articles. The following steps illustrates the procedure followed in retrieving data from the search queries:

- Enter key search phrases.
- Separate each key search phrase with “AND”
- Refine search by selecting “subscribed journals”.
- Select data sources to “conference, books, journals, magazines and journal articles”.
- Select all years.
- Extract data to Endnote through downloading RIS files.

**Table 6: ScienceDirect data extraction summary**

| **Search string 1** | *Employees **AND** cybersecurity culture challenges **AND** Cybersecurity knowledge requirement **AND** Critical Infrastructure* | | | | | | |
|---|---|---|---|---|---|---|---|
| **Source type** | Journal Article | Conference paper | Book section | Article in Press | Magazine | Thesis | Total |
| **Results** | 127 | 2 | | 4 | | | 133 |
| **Search string 2** | *Employees **AND** cybersecurity awareness problems **AND** Cybersecurity education and training **AND** Critical Infrastructure* | | | | | | |
| **Source type** | Journal Article | Conference paper | Book section | Article in Press | Magazine | Thesis | Total |
| **Results** | 122 | 2 | | 3 | | | 127 |

UNIVERSITY OF JOHANNESBURG

## Screening for removing duplicates

Screening for duplicates was done by making use of DOI numbers to identify duplicate articles from different databases. The identified duplicates were removed with the help of Endnote and by verifying duplicates through screening the DOI numbers of each document. A total of 633 duplicates were found and 1380 distinctive document titles remains.

The total 1380 remaining document tiles are categorised as follows:

- Journal article :963
- Conference paper :271
- Book section :138
- Article in Press :6
- Magazine :

**Table 7: Summary of remaining distinctive document titles**

| | | Data source | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Journal Article | Conference paper | Book section | Article in Press | Magazine | Thesis | **Total** |
| **Database** | ProQuest | 492 | | | | 2 | | 494 |
| | IEEE | 67 | 82 | 57 | | | | 206 |
| | Emerald | 141 | | 7 | | | | 148 |
| | Engineering Village | 65 | 189 | 11 | 1 | | | 266 |
| | Wiley Online | 11 | | 63 | | | | 74 |
| | ScienceDirect | 187 | | | 5 | | | 192 |
| | **Total** | 963 | 271 | 138 | 6 | 2 | | 1380 |

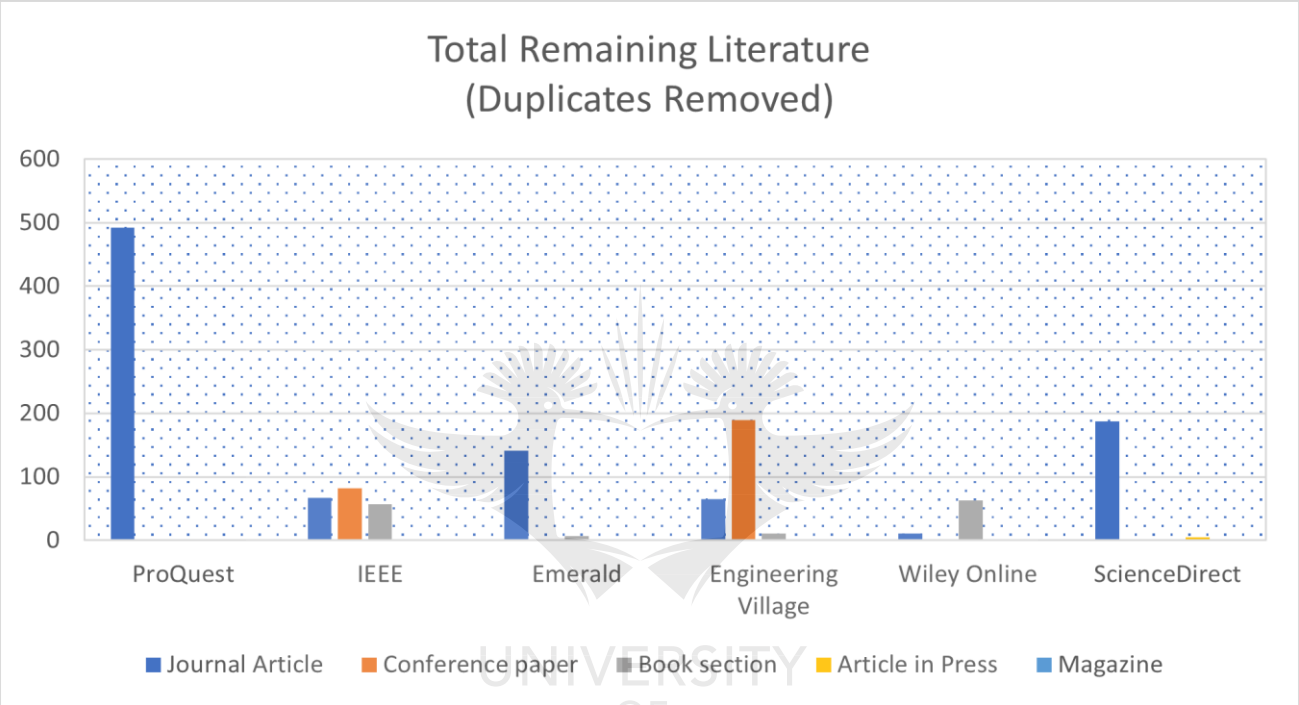


**Figure 6: Total remaining literature**

UNIVERSITY OF JOHANNESBURG

# APPENDIX B

The selected documents are detailed in tables below with author, document title and publication date and resulting word codes.

**Table 8: ProQuest selected documents and resulting word codes.**

| Author | Title | Pub. Year | No. of Hits |
|---|---|---|---|
| | Cybersecurity Challenges in Industry: Measuring the Challenge Solve Time to Inform Future Challenges. | 2020 | 25 |
| Rosner, E. | Cyber Federalism: Defining Cyber's Jurisdictional Boundaries. | 2017 | 100 |
| Reed, T. | You Can't Always Get What You Want: Employee and Organizational Responses to Perceived Workplace Injustices and their Relationship to Insider Attacks. | 2019 | 74 |
| Ani, U. D., H. He and A. Tiwari | Human factor security: evaluating the cybersecurity capacity of the industrial workforce. | 2019 | 57 |
| Eichensehr, K. E. | Public-Private Cybersecurity. | 2017 | 53 |
| Dunn, K. | The Oregon Trail: An Exploratory Case Study for Higher Education Emergency Management Programs. | 2018 | 52 |
| Crowell, B. | Maritime Homeland Security and the Role of Area Maritime Security Committees. | 2018 | 51 |
| Asllani, A., C. S. White and L. Ettkin | VIEWING CYBERSECURITY AS A PUBLIC GOOD: THE ROLE OF GOVERNMENTS, BUSINESSES, AND INDIVIDUALS. | 2013 | 26 |
| Fox, A. | Putting the Lid on the Devil's Toy Box: How the Homeland Security Enterprise Can Decide Which Emerging Threats to Address. | 2018 | 49 |
| Limba, T., T.Plėta, K.Agafonov and M. Damkus | Cyber security management model for critical infrastructure. | 2018 | 48 |
| Chaturvedi, M., A. Narain Singh, M. Prasad Gupta and J. Bhattacharya | Analyses of issues of information security in the Indian context. | 2014 | 44 |
| Korta, S. | Fake News, Conspiracy Theories, and Lies: An Information Laundering Model for Homeland Security. | 2017 | 42 |
| Mihaela, C. L. | Current security threats in the national and international context. | 2020 | 40 |
| Cooke, J. | Measuring State Resilience: What Makes a Difference? | 2018 | 39 |
| Molinari, M. | Implementing CompStat Principles Into Critical Infrastructure Protection and Improvement. | 2016 | 39 |
| Dlamini, S. and C. Mbambo | Understanding policing of cyber-crime in South Africa: The phenomena, challenges and effective responses. | 2019 | 25 |
| Ghadge, A., M. Weiß, N. D. Caldwell and R. Wilding | Managing cyber risk in supply chains: a review and research agenda. | 2019 | 38 |
| Adane, K. | The Current Status of Cyber Security in Ethiopia. | 2020 | 35 |
| Knopf, K. | Fully Autonomous Vehicle Borne Improvised Explosive Device—Mitigating Strategies. | 2019 | 35 |
| Pawlowski, S. D. and Y. Jung | Social Representations of Cybersecurity by University Students and Implications for Instructional Design. | 2015 | 35 |
| Mambile, C. and P. Mbogoro | Cybercrimes awareness, cyber laws and its practice in public sector Tanzania. | 2020 | 34 |

UNIVERSITY OF JOHANNESBURG

| | | | |
|---|---|---|---|
| Bozkus Kahyaoglu, S. and C. Kiymet | Cyber security assurance process from the internal audit perspective. | | 33 |
| Zhang, Z. | NERC's Cybersecurity Standards for the Electric Grid. | 2011 | 33 |
| Kannan, K. S. P. and A. Garad | Competencies of quality professionals in the era of industry 4.0: a case study of electronics manufacturer from Malaysia. | 2020 | 32 |
| Stewart, C. A. | Full Court Press: Preventing Foreign Adversaries from Exfiltrating National Security Technologies Through Bankruptcy Proceedings. | 2019 | 32 |
| Mustafa, S. and E. Karacuha | Creating and Implementing an Effective and Deterrent National Cyber Security Strategy. | 2020 | 31 |
| Wolfe, A. | Unstoppable? The Gap Between Public Safety and Traffic Safety in the Age of the Driverless Car. | 2017 | 30 |
| Bada, M. and J. R. C. Nurse | Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). | 2019 | 29 |
| Claus, B., R. A. Gandhi, J. Rawnsley and J. Crowe | Using the Oldest Military Force for the Newest National Defense. | 2015 | 29 |
| Lis, P. and J. Mendel | Cyberattacks on critical infrastructure: An economic perspective. | 2019 | 29 |
| Sekuloski, M. | SECURITY SECTOR REFORM WISDOM FOR CYBER SECURITY INSTITUTION BUILDING: THE CASE OF SERBIA. | 2016 | 29 |
| Smith, M. and G. Mulrain | Equi-failure: The National Security Implications of the Equifax Hack and a Critical Proposal for Reform. | 2017 | 29 |
| Adams, M. and M. Makramalla | Cybersecurity Skills Training: An Attacker-Centric Gamified Approach. | 2015 | 27 |
| Carlton, M., Y. Levy and M. Ramin | Mitigating cyber-attacks through the measurement of non-IT professionals' cybersecurity skills. | 2019 | 27 |
| Gibbs, T. | Seeking economic cyber security: a Middle Eastern example. | 2020 | 27 |
| Pawlak, P. and C. Wendling | Trends in cyberspace: can governments keep up? | 2013 | 27 |
| Harris, M. A. and K. P. Patten | Mobile device security considerations for small- and medium-sized enterprise business mobility. | 2014 | 27 |
| Kandasamy, K., S. Sethuraman, K. Achuthan and V. P. Rangan | IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. | 2020 | 27 |
| | A Systematic Review of Cybersecurity Risks in Higher Education. | 2021 | 26 |
| Abeyratne, R. | Cyber terrorism and aviation--national and international responses. | 2011 | 26 |
| Doynikova, E., E. Novikova and I. Kotenko | Attacker Behaviour Forecasting Using Methods of Intelligent Data Analysis. | 2020 | 26 |
| Linkov, I., D. A. Eisenberg, K. Plourde, T. P. Seager, J. Allen and A. Kott | Resilience metrics for cyber systems. | 2013 | 26 |
| Al-Hamdani, W. A. P. | Education Organization Baseline Control Protection and Trusted Level Security. | 2007 | 25 |
| Tasevski, P. | IT AND CYBER SECURITY AWARENESS-RAISING CAMPAIGNS. | 2016 | 25 |
| Masike, M., S. Sune Von and A. Marnewick | Socio-technical systems cybersecurity framework. | 2019 | 25 |
| Sevan, G. | A Proposed Cosmology of Identity in The Sociotechnical Ecosystem of Homeland Security. | 2017 | 25 |

UNIVERSITY OF JOHANNESBURG

**Table 9: IEEE selected documentsand resulting word codes**

| Author | Title | Pub. Year | No. of Hits |
|---|---|---|---|
| Ahrend, J. M., M. Jirotka and K. Jones | On the collaborative practices of cyber threat intelligence analysts to develop and utilize tacit Threat and Defence Knowledge. | 2016 | 32 |
| Al-Enezi, K. A., I. F. Al-Shaikhli, A. R. Al-Kandari and S. S. M. Aldabbagh | Cyber-Attacks Detection & Protection in Kuwait Government Sectors. | 2014 | 25 |
| Alissa, K. A., H. A. Alshehri, S. A. Dahdouh, B. M. Alsubaie, A. M. Alghamdi, A. Alharby and N. A. Almubairik | An Instrument to Measure Human Behavior Toward Cyber Security Policies. | 2018 | 26 |
| Deursen, N. E. V. | Visual Communication for Cybersecurity: Beyond Awareness to Advocacy. | 2019 | 25 |
| Dorasamy, M., G. C. Joanis, L. W. Jiun, M. Jambulingam, R. Samsudin and N. J. Cheng | Cybersecurity Issues Among Working Youths in an IoT Environment: A Design Thinking Process for Solution. | 2019 | 25 |
| Elisa, B. | Data Protection from Insider Threats. | 2012 | 26 |
| Elkhannoubi, H. and M. Belaissaoui | A framework for an effective cybersecurity strategy implementation: Fundamental pillars identification. | 2015 | 27 |
| Galinec, D. and W. Steingartner | Combining cybersecurity and cyber defence to achieve cyber resilience. | 2017 | 40 |
| Hunter, A. and D. Leversage | Building a Curriculum for Industrial Network Security. | 2019 | 25 |
| Isaac, P. | Cyberwarfare: An Introduction to Information-Age Conflict. | 2019 | 34 |
| Jeong, J. J., M. Grobler, M. A. P. Chamikara and C. Rudolph | Fuzzy Logic Application to Link National Culture and Cybersecurity Maturity | 2019 | 26 |
| Kianpour, M., S. Kowalski, E. Zoto, C. Frantz and H. Øverby | Designing Serious Games for Cyber Ranges: A Socio-technical Approach | 2019 | 25 |
| Losavio, M., J. Hinton, K. Fritz, A. Lauf, J. Hieb, G. Im, A. Wright, J. Reed, A. Elmaghraby, D. Keeling, J. Gainous, J. Sun and M. Bergman | STEM for Public Safety in Cyber: Training for Local Law Enforcement and Cyber Security | 2019 | 27 |
| Mulyadi and D. Rahayu ( | Indonesia National Cybersecurity Review: Before and After Establishment National Cyber and Crypto Agency | 2018 | 27 |
| Nagarajan, A., J. M. Allbeck, A. Sood and T. L. Janssen | Exploring game design for cybersecurity training | 2012 | 28 |
| Paulsen, C., E. McDuffie, W. Newhouse and P. Toth | NICE: Creating a Cybersecurity Workforce and Aware Public | 2012 | 34 |
| Persadha, P. D., A. A. Waskita, M. I. Fadhila, A. Kamal and S. Yazid | How does inter-organizational knowledge sharing drive national cyber security awareness?: A case study in Indonesia | 2016 | 30 |
| Rege, A. | Incorporating the human element in anticipatory and dynamic cyber defence | 2016 | 27 |
| Rege, A., T. Nguyen and R. Bleiman | A social engineering awareness and training workshop for STEM students and practitioners | 2020 | 30 |
| Subramanian, R. | Historical Consciousness of Cyber Security in India | 2020 | 32 |
| Turkanović, M., T. Welzer and M. Hölbl | An Example of a Cybersecurity Education Model | 2019 | 25 |

UNIVERSITY OF JOHANNESBURG

| | | | |
|---|---|---|---|
| Wang, Z., H. Zhu and L. Sun | Social Engineering in Cybersecurity | 2021 | 26 |
| Veiga, A. D. | A cybersecurity culture research philosophy and approach to developing a valid and reliable measuring instrument | 2016 | 32 |
| Wei, W., A. Mann, K. Sha and T. A. Yang | Design and implementation of a multi-facet hierarchical cybersecurity education framework | 2016 | 28 |
| Yardley, T., S. Uludag, K. Nahrstedt and P. Sauer | Developing a Smart Grid cybersecurity education platform and a preliminary assessment of its first application | 2014 | 29 |

**Table 10: Emerald selected documentsand resulting word codes.**

| Author | Title | Pub. Year | No. of Hits |
|---|---|---|---|
| A. Harris, M. and K. P. Patten | Mobile device security considerations for small- and medium-sized enterprise business mobility | 2014 | 27 |
| Ahmad, Z., T. S. Ong, T. H. Liew and M. Norhashim | Security monitoring and information security assurance behaviour among employees | 2019 | 66 |
| AlMindeel, R. and J. T. Martins | Information security awareness in a developing country context: insights from the government sector in Saudi Arabia | 2020 | 31 |
| Bozkus Kahyaoglu, S. and K. Caliyurt | Cyber security assurance process from the internal audit perspective | 2018 | 33 |
| Campbell, C. C | Solutions for counteracting human deception in social engineering attacks | 2019 | 31 |
| Caron, F. | Obtaining reasonable assurance on cyber resilience | 2019 | 25 |
| Dedeke, A. and K. Masterson | Contrasting cybersecurity implementation frameworks (CIF) from three countries | 2019 | 26 |
| Kannan, K. S. P. N. and A. Garad | Competencies of quality professionals in the era of industry 4.0: a case study of electronics manufacturer from Malaysia | 2020 | 32 |
| Karagiannis, S. and E. Magkos | Adapting CTF challenges into virtual cybersecurity learning environments | 2020 | 42 |
| Kumar, S., B. Biswas, M. S. Bhatia and M. Dora | Antecedents for an enhanced level of cyber-security in organisations | 2020 | 30 |
| Mugarura, N. and E. Ssali | Intricacies of anti-money laundering and cyber-crimes regulation in a fluid global system | 2020 | 31 |
| Pérez-González, D., S. T. Preciado and P. Solana-Gonzalez | Organizational practices as antecedents of the information security management performance | 2019 | 27 |
| Ramlo, S. and J. B. Nicholas | The human factor: assessing individuals' perceptions related to cybersecurity | 2021 | 28 |
| Saban, K. A., S. Rau and C. A. Wood | SME executives' perceptions and the information security preparedness model | 2021 | 29 |
| Sadok, M., S. Alter and P. Bednar | It is not my job: exploring the disconnect between corporate security policies and actual security practices in SMEs | 2020 | 30 |
| Sallos, M. P., A. Garcia-Perez, D. Bedford and B. Orlando | Strategy and organisational cybersecurity: a knowledge-problem perspective | 2019 | 27 |
| Shah, M., A. Maitlo, P. Jones and Y. Yusuf | An investigation into agile learning processes and knowledge sharing practices to prevent identity theft in the online retail organisations | 2019 | 36 |
| hah, P. and A. Agarwal | Cybersecurity behaviour of smartphone users in India: an empirical analysis | 2020 | 43 |
| Zhang, Z., W. He, W. Li and M. H. Abdous | Cybersecurity awareness training programs: a cost-benefit analysis framework | 2021 | 25 |

**Table 11: Engineering Village selected documentsand resulting word codes.**

| Author | Title | Pub. Year | No. of Hits |
|---|---|---|---|
| | 5th World Conference on Information Security Education | 2007 | 32 |
| | 32nd International Conference on Information System 2011 | 2011 | 40 |

| | | | |
|---|---|---|---|
| | 2nd International Workshop on Information and Operational Technology | 2020 | 43 |
| Al Ghazal, M. A. and M. J. Al Jubran | Cybersecurity for upstream operations | 2017 | 39 |
| Al Jahil, A. A. and D. Giarratano | Improvement of cyber-security measures in National Grid SA substation process control | | 29 |
| Amaba, B. | Industrial and business systems for Smart Cities | 2014 | 36 |
| Astakhova, L. and I. Medvedev | The Software Application for Increasing the Awareness of Industrial Enterprise Workers on Information Security of Significant Objects of Critical Information Infrastructure | 2020 | 26 |
| Ataei, H. and O. M. Salem | Construction regulations and organizational management | 2016 | 31 |
| Bernik, I. and K. Prislan | Cyber terrorism in Slovenia-fact or fiction | 2011 | 29 |
| Bohm, F., M. Vielberth and G. Pernul | Bridging knowledge gaps in security analytics | 2021 | 33 |
| Boranbayev, A., S. Boranbayev and A. Nurbekov | Measures to ensure the reliability of the functioning of information systems in respect to state and critically important information systems | 2021 | 32 |
| Carroll, J. | Offensive and defensive cyberspace operations training: Are we there yet? | 2018 | 35 |
| Catota, F. E., M. Granger Morgan and D. C. Sicker | Cybersecurity education in a developing nation: The Ecuadorian environment | 2019 | 45 |
| Chileshe, G. and R. V. Heerden | SCADA systems in South Africa and their vulnerabilities | 2012 | 25 |
| Daniel Ani, U. P., H. M. He and A. Tiwari | Human capability evaluation approach for cyber security in critical industrial infrastructure | 2016 | 33 |
| Davidson, L. | Defining the workforce and training array for the cyber risk management and cyber resilience methodology of an army | 2020 | 43 |
| Dominguez, M., A. Moran, S. Alonso, M. A. Prada, D. Perez and J. J. Fuertes | Experimentation environment for industrial control systems cybersecurity: On-site and remote training | 2019 | 25 |
| Dominguez, M., M. A. Prada, P. Reguera, J. J. Fuertes, S. Alonso and A. Moran | Cybersecurity training in control systems using real equipment | 2017 | 34 |
| Erdogan, G., A. a. Romero, N. Zazzeri, A. itnik, M. Basile, G. Aprile, M. Osorio, C. Pani and I. Kechaoglou | Developing cyber-risk centric courses and training material for cyber ranges: A systematic approach | 2021 | 25 |
| Feng, W.-C., R. Liebman, L. Delcambre, M. Lupro, T. Sheard, S. Britell and G. Recktenwald | A camp for broadening participation in cybersecurity | 2017 | 28 |
| Ficco, M. and F. Palmieri | Leaf: An open-source cybersecurity training platform for realistic edge-IoT scenarios | 2009 | 29 |
| Flanagan, E., C. Carlson and R. Stencel | Successful procedure for wastewater bypass in the heart of Dallas | 2020 | 40 |
| Galloway, P. | The 21st-century engineer | 2008 | 53 |
| Gisladottir, V., A. A. Ganin, J. M. Keisler, J. Kepner and I. Linkov | The resilience of Cyber Systems with Over- and Underregulation | 2017 | 25 |
| Goeke, L., A. Quintanar, K. Beckers and S. Pape | PROTECT An Easy Configurable Serious Game to Train Employees Against Social Engineering Attacks | 2020 | 25 |
| Greiman, V. and L. Chitkushev | Legal frameworks to confront cybercrime: A global academic perspective | 2011 | 31 |

UNIVERSITY OF JOHANNESBURG

| | | | |
|---|---|---|---|
| Jin, G., M. Tu, T.-H. Kim, J. Heffron and J. White | Game-based cybersecurity training for High School Students | 2018 | 34 |
| Karabacak, B., S. Ozkan Yildirim and N. Baykal | Regulatory approaches for the cyber security of critical infrastructures: The case of Turkey | | 34 |
| Karamouz, M., S. Saadati and A. Ahmadi | Vulnerability assessment and risk reduction of water supply systems | 2020 | 26 |
| Khan, A. H., P. B. Sawhney, S. Das and D. Pandey | SartCyber Security Awareness Measurement Model | 2020 | 27 |
| Krumay, B., E. W. N. Bernroider and R. Walser | Evaluation of Cybersecurity Management Controls and Metrics of Critical Infrastructures: A Literature Review Considering the NIST Cybersecurity Framework | 2018 | 27 |
| Kunicina, N., A. Zabasta, O. Krumins, A. Romanovs and A. Patlins | Cybersecurity Curricula Recommendations Development for Technical Background and Engineering Skills in International Dimension | 2020 | 38 |
| Liphadzi, S. M. and A. P. Vermaak | Assessment of employees' perceptions of approaches to sustainable water management by coal and iron ore mining companies | 2017 | 31 |
| Macher, G., R. Messnarz, E. Armengaud, A. Riel, E. Brenner and C. Kreiner | Integrated Safety and Security Development in the Automotive Domain | 2017 | 25 |
| Mahoney, W. and R. A. Gandhi | An integrated framework for control system simulation and regulatory compliance monitoring | 2011 | 25 |
| Marek, J. A. | Cybersecurity and risk management framework in avionics | 2018 | 35 |
| Martin, A. and L. C | An intelligent e-learning scenario for knowledge retrieval | 2012 | 29 |
| Martin, A. and C. Leon | An intelligent e-learning scenario for knowledge retrieval | 2012 | 29 |
| Martin, T. and G. F. Rylander | Innovative approaches to enhancing transportation operations, Institute of Transportation EngineersAs stated at the beginning of this article, there were four recurring themes throughout the presentations | 2009 | 28 |
| Nader, P., P. Honeine and P. Beauseroy | Intrusion detection in SCADA systems using one-class classification | 2013 | 25 |
| Nader, P., P. Honeine and P. Beauseroy | Detection of cyberattacks in a water distribution system using machine learning techniques | 2016 | 27 |
| Newberg, R. and J. Sendra | Proactive planning provides a roadmap for water reclamation sustainability | 2015 | 49 |
| Patrascu, A. and E. Simion | Cyber security evaluation of critical infrastructures systems, Nova Science Publishers, | 2014 | 36 |
| Pawlowski, S. D. and Y. Jung | Social representations of cybersecurity by university students and implications for instructional design | 2015 | 36 |
| Pettersen, K. A. and T. Bjornskau | Organizational contradictions between safety and security - Perceived challenges and ways of integrating critical infrastructure protection in civil aviation | 2015 | 28 |
| Prins, S., A. Marnewick and S. von Solms | Cybersecurity awareness in an industrial control systems company | 2020 | 26 |
| Rajamaki, J., J. Nevmerzhitskaya and C. Virag | Cybersecurity education and training in hospitals: Proactive resilience educational framework | 2018 | 36 |
| Rappel, R., J. Dorscht and R. Sahney | The application of a knowledge transfer taxonomy to pipeline construction inspection best practices | 2018 | 26 |
| Rege, A. and J. Adams | The need for more sophisticated cyber-physical systems war gaming exercises | 2019 | 26 |
| Riley, D. M. and J. L. Hall | Privatization of public education: Lessons from New Orleans for engineering education in K-12 and beyond | 2016 | 37 |
| Sample, C., S. M. Loo and M. Bishop | Resilient data: An interdisciplinary approach. 2020 Resilience Week | 2020 | 30 |

UNIVERSITY OF JOHANNESBURG

| | | | |
|---|---|---|---|
| Spremi, M. and A. imunic | Cyber security challenges in the digital economy | 2018 | 38 |
| Subhani, N. A., M. Z. Iqbal and M. M. Khan | Business continuity and crisis management | 2016 | 36 |
| Tsegaye, T. and S. Flowerday | Controls for protecting critical information infrastructure from cyberattacks | 2014 | 29 |
| Turkanovi, M., T. Welzer and M. Holbl | An example of a cybersecurity education model | 2019 | 25 |
| Vakova, M. and J. Barta | Training of the critical infrastructure employees | 2017 | 26 |
| Van Eeten, M. J. G., H. De Bruijn, M. Kars, H. Van Der Voort and J. Van Till | The governance of cybersecurity: A framework for policy | 2006 | 25 |
| Varga, S., J. Brynielsson and U. Franke | Information requirements for national-level cyber situational awareness. | 2018 | 25 |
| Vivero, J. and L. Ripoll | Cyber situational awareness in space organizations operations centres | 2018 | 51 |

**Table 12: ScienceDirect selected documentsand resulting word codes.**

| Author | Title | Pub. Year | No. of Hits |
|---|---|---|---|
| Bryan, E., A. Larsen, I. Brass and J. H. Sowell | Best Practices of the Board of DirectorsCybersecurity Policies and Procedures | 2017 | 32 |
| Busby, J. S., B. Green and D. Hutchison | Your Cybersecurity ProgramnAnalysis of Affordance, Time, and Adaptation in the Assessment of Industrial Control System Cybersecurity Risk | 2019 | 28 |
| Clark, R. M., S. Panguluri, T. D. Nelson and R. P. Wyman | Protecting Drinking Water Utilities from Cyberthreats | 2017 | 26 |
| Gcaza, N. and R. von Solms | A Strategy for a Cybersecurity Culture: A South African Perspective | 2017 | 25 |

**Table 12: ScienceDirect selected documentsand resulting word codes.**

| Author | Title | Pub. Year | No. of Hits |
|---|---|---|---|
| Ali, O., A. Shrestha, A. Chatfield and P. Murray | Assessing information security risks in the cloud: A case study of Australian local government authorities | 2020 | 30 |
| Alladi, T., V. Chamola and S. Zeadally | Industrial Control Systems: Cyberattack trends and countermeasures. | 2020 | 25 |
| Alshaikh, M. | Developing cybersecurity culture to influence employee behaviour: A practice perspective | 2020 | 26 |
| Cascavilla, G., D. A. Tamburri and W.-J. Van Den Heuvel | Cybercrime threat intelligence: A systematic multi-vocal literature review | 2021 | 27 |
| Chowdhury, N. and V. Gkioulos | Cyber security training for critical infrastructure protection: A literature review | 2021 | 26 |
| Givens, A. D. and N. E. Busch | Realizing the promise of public-private partnerships in U.S. critical infrastructure protection | 2013 | 29 |
| Goodman, S. E., J. C. Kirk and M. H. Kirk | Cyberspace as a medium for terrorists | 2007 | 26 |
| Karabacak, B., S. O. Yildirim and N. Baykal | A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness | 2016 | 41 |
| Malatji, M., A. Marnewick and S. von Solms | Validation of a socio-technical management process for optimising cybersecurity practices | 2020 | 27 |
| Manning, L. | Food defence: Refining the taxonomy of food defence threats | 2019 | 26 |
| Srinivas, J., A. K. Das and N. Kumar | Government regulations in cyber security: Framework, standards and recommendations | 2019 | 38 |
| Torten, R., C. Reaiche and S. Boyle | The impact of security awareness on information technology professionals' behaviour | 2018 | 27 |

UNIVERSITY OF JOHANNESBURG

| | | | |
|---|---|---|---|
| Zimmermann, V. and K. Renaud | Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset | 2019 | 31 |

UNIVERSITY OF JOHANNESBURG